"Biometrics and the Digital Borders of the EU. Where is Europe heading?"

MA Thesis European Studies
Graduate School for Humanities
Universiteit van Amsterdam

Author: Eleni Kanava
Main Supervisor: Marieke de Goede
Second Supervisor: Menno Spiering

February 2010

Abstract

In recent years, heightened security concerns arising from the increase of transnational terrorism and crime have affected the ways in which governments in the international arena approach border security issues. As a direct result of these concerns, migratory flows have increasingly come to be seen as a non-traditional security threat to nation states which are in turn held accountable for developing more effective migration management systems as a response to security considerations. A key aspect of this new approach has been to tighten control of borders, to ensure safer travel documents as well as to promote enhanced cooperation on migration issues among states in the international stage.

However, the most crucial component in reinforcing security measures for the control of migratory flows consists the introduction of biometric systems in various domains of migration management. More specifically, biometric applications are increasingly being conceptualized and progressively implemented aiming at increasing safety, interoperability, availability and efficient border controls. This is mostly evident in EU migration policies where biometrics are becoming increasingly developed and enacted resulting in the mass collection and storage of biometric data not only in relation to third-country nationals seeking entry into the EU but also to the EU nationals through the development of e-passports.

In this regard, the development of biometric technologies has given rise to considerable concerns amongst privacy and civil liberties proponents who reveal the legal repercussions of biometrics as an "anchor". More specifically, they strongly affirm that there are important human rights and legal implications inherent in the collection, processing, and distribution of a person's unique physical identifiers, causing a certain degree of friction between the security interests of policymakers and the civil liberties of those subject to any of these measures. Indeed, this friction is at the heart of the biometrics debate (Rebekah 2005, p. 2).

It is evident then that the use of biometrics is at the centre of the international migration agenda and therefore an interesting case through which to examine future developments in EU's migration policies. Building up from the introduction of biometrics in EU's migration policies and the increasing digitalization of EU's borders, this dissertation will address the legal limits and rising civil concerns over the use of biometrics as part of an ever-increasing securitization of migratory flows.

Contents

Introduction

It is generally maintained that in the aftermath of the terrorist attacks of 9/11, international actors have undoubtedly changed their approach in border security issues and have increased their interest in the deployment of biometric technologies as an answer to potential terrorist threats (Heisler 2006; Huysmans 2006; Boswell 2007). A recent attempted terrorist attack on 25 December 2009 by a would-be bomber who boarded a flight from Amsterdam to Detroit has further intensified the debate on biometrics and their potential advantages on combating terrorism (BBC News, 28 December 2009). Questions as to how did a person who was on an American watch-list manage to slip through the many nets that should have been in place to prevent him reveal not only the failure of US and EU intelligence in addressing potential terrorist threats, but also how biometrics are increasingly been seen as the most appropriate answer to security concerns. More specifically, in the wake of the alleged attempt to bomb a Detroit-bound plane, the EU member states have been under considerable pressure from the US to adopt more strict security measures at the airports by installing body scanners to be used obligatorily to all passengers traveling to the US. In response to these developments, the Netherlands and the United Kingdom have since announced that they will install body scanners and within three weeks all US-bound passengers will be required to pass through these biometric machines at their international airports (New York Times, 7 January 2010). Indeed, Amsterdam's airport authorities that have already in their possession fifteen body scanners and their use until now has only been on a voluntary basis, have recently advocated the extensive use of these scanners on all flights passengers (NRC 22 January 2010). In contrast, some of the EU's member states, including Germany, remain rather reluctant considering that the relevant technology not only violates the privacy of passengers – body scanners produce an image of a traveler's naked body – but also could be considered as the source of potential health hazards (Spiegel 30 December 2009). Hence, EU member states remain rather divided on the use of biometric technologies at the airports revealing not only the complex and contradictory nature of these technologies, but also the increasing ethical and normative concerns over their extensive use. It is clear that the use of body scanners is increasingly been seen as the answer to terrorist threats but their ability to detect and prevent such threats still remains to be proved.

In the light of these developments, the introduction of biometric technologies have given rise to considerable concerns amongst privacy and civil rights advocates and have

fostered a political and academic debate on the role of biometrics in migration management. To that extent, many questions concerning not only the potential technical dangers deriving from the use of biometrics but also the potential social implications of biometric databases such as those currently being established at the EU level are arising. How is the use of biometric technologies going to change previous migratory regimes? What will be the impact on mobile populations? Do international actors such as the EU have a clear vision of where this accumulation of personal data could lead to? Could it lead to a massive collection of data with an unknown future of potential use or abuse? Which civil liberties could be endangered and how will rising legal concerns be dealt with? This dissertation will address these questions by starting off with a technological overview of biometrics in order to offer a general understanding of today's biometric techniques and applications.

Chapter 1

Understanding Biometrics: A Technological Overview

It is generally maintained that states responses to new security threats have become more sophisticated over the years and far reaching, employing highly technical, increasingly punitive and innovative methods (Pickering & Weber 2006, p. 9). Among these methods evolving new forms of surveillance, transaction, data generating, gathering and commodification, biometrics have came to be described as "the next best thing in information technology" (Van der Ploeg 1999, p. 37). In fact, they can be used as a means of proving that you are who you claim to be, or as a means of proving without revealing your identity that you have a certain right (e.g. access), just like a PIN (personal identification number) or a password (European Commission 2005a, p. 35). The crucial difference however between biometrics and technological applications such as the PIN is that the former is something that is part of your body, rather than something you know or can carry with you (Hopkins, 1999).

Current applications of biometrics are multipurpose, ranging from regulation of asylum and migration, to electronic patients records, access by personnel to sensitive areas of governmental or commercial buildings, on to aviation security and fight against terrorism (Liberatore 2005, p. 4). In order to better understand the challenges posed by biometric technologies and its various applications, this chapter provides some background information on the main technological issues of biometric systems, independent of the technology used or purposes served.

1.1 Biometrics as Technology

The term biometrics (from the Greek *bios*: life and *metron*: measurement) has multiple meanings and is defined here as the automated means of identifying an individual through the measurement of distinguishing physiological-biological characteristics or behavioural traits (Liberatore 2005, p. 3; Redpath 2005, p. 6).). Physiological characteristics include fingerprints, hand geometry, iris shape, face, voice, ear shape, and body odor. Behavioural traits include mainly hand-written signatures (Rebekah 2005, p. 1).

As far as the features of biometric identification are concerned, biometric technology involves the collection with a sensoring device of digital representations of physiological or behavioural traits that are in turn transformed via some algorithm to produce a "template" (European Commission 2005b, p. 12). This algorithmic transformation that is said to be irreversible produces a template that is usually stored in centralized databases, accessed when for example a finger, hand, face, eye or voice is presented to the system (Van der Ploeg 2007, p. 47). If a matching template is found, the persons presenting themselves are "recognized" and count as "known" to the system. Hence, most biometric systems are based on mathematical formulae to detect statistically significant correlations between a live-capture biometric and biometric templates previously entered into computer system (Redpath 2005, p.7).

To sum up, biometric identification works in four stages: enrolment, storage, acquisition, matching. Firstly, individuals are enrolled and a record associating the identifying features with the individual is created. There are two options for storage: the records can be stored in a central database, or in a decentralized way, for example on smart cards or tokens. Thirdly, when identification is required, a new sample of the feature is acquired. Finally, the newly acquired record is compared to the stored record and if they match, the individual has been identified (Jain et al. 2008, p. 5).

1.2 Biometric Utilities

In functional terms, the current uses of biometrics can be categorized under the following headings: verification and identification (Sprokkereef 2008, p. 278). As far as verification is concerned, biometric verification requires comparing a registered or enrolled biometric sample against a newly captured biometric sample (Varra 2007, p. 24). To put it simply, biometric reading can be used to verify that an individual is who he/she claims to be. More specifically, this involves a one-to-one match between a subject's biometric data obtained at the point of verification and a biometric template created when the subject enrolled in the system (Ashbourn 2000, p. 13). For instance, once biometric is included in a travel document, whether visa or passport or identification card, the person holding that document can be checked through live-capture against the biometric data stored in the document (Schouten et al. 2009, p. 306). It is clear then that the searching process in on-to-

one as the biometric is used to verify that the person is the same in the document application record, or presented in the passport or travel document.

As far as the biometric use of identification is concerned, the latter is used to identify individuals when one-to-one is either not possible or sufficient. More specifically, this involves a one-to-many search between a subject's biometric data, which can be either live-captured or from another source, and a collection of templates of the same biometric of all the individuals enrolled in the system (Sethi 2004, p. 108). To sum up, of the two alternatives of verification and identification, one-to-one matches have the highest rate of accuracy. However, the technology behind one-to-many searches is improving and the use of multi-tiered biometric searching (searching more than one biometric identifier in a certain sequence) is one way of increasing the accuracy of these searches (Woodward et al. 2004, p. 8).

1.3 Biometric Techniques

In fact, there are various biometric techniques that are used for verification and identification processes. They mostly involve fingerprinting, iris recognition, facial recognition, hand geometry, voice recognition and signature verification (Ashbourn 2004, p. 5-6).

As far as fingerprinting technology is concerned, this technique involves the placing of finger/s on an electronic scanner that reads the unique ridges on the finger (Kumar et al. 2009, p. 28). More specifically, this biometric technology uses the pattern of friction ridges and valleys on an individual's fingertips that are considered unique to a specific individual (Poli et al. 2009, p.262). Fingerprints are then matched by the comparison if the position of minutiae points or by a more general matching approach (Ashbourn 2004, p. 5). Fingerprint devices tend to be based upon either optical readers or capacitive based chips. This variation of both fundamental matching principles and capture mechanisms provides for an interesting variety of devices but does raise questions about true interoperability (Ashbourn 2004, p. 5).

In the cases of iris-scanning and retina scanning, it is important to notice that while iris scanning involves the photographic scanning of the unique coloured patterns of the iris, retina scanning is based on the examination of the blood vessels at the retina that provide a

unique pattern, which may be used as a tamper-proof personal identifier (Leonidou 2002, p. 8; Spinella 2003, p. 8). Iris and retina scans are considered as the most accurate but also as the most invasive forms of identification that are often implemented at various airports worldwide for passenger authentication in frequent flier services. (Wade 2004, p. 76).

On the account of facial recognition technology, this kind of biometric technique is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. Regardless of specific method used, facial recognition is accomplished in a five- step process (Woodward et al. 2003, p. 8). Over the years, this technique has been supplemented by the development of 3D variants and other techniques such as surface texture analysis and has proven to be a viable biometric method.

Lastly, hand geometry is one of the longer running biometric techniques and there are large numbers of devices in regular operation around the world (Kumar et al 2003, p. 671). Hand geometry, as the name suggests, refers to the geometric structure of the hand. This structure includes width of the fingers at various locations including the width of the palm, thickness of the palm and length of the finger. (Ross & Jain 2003, p. 2120). Although these metrics do not vary significantly across a population, they can nevertheless be used to verify the identity of an individual (Wade 2004, p. 76). This technique is currently implemented in some countries such as Israel as a form of border control that is used as a brief scanning of the hand to verify the subject's identity (Lyon 2001 in Wade 2003, p. 76). Hence, hand-geometry is a non-intrusive measurement and the verification involves a single processing of the resulting features (Ross &Jain 2003, p. 2120).

1.4 Conclusion

To sum up, it is generally contested that the most reliable biometric features are fingerprinting and iris scanning both in one-to-one matching and one-to-many matches and are the most frequently used in migration management (Redpath 2005, p. 7). However, the International Civil Aviation Organization (ICAO), the international organization leading the setting of standards for the use of biometrics in passports, have concluded that face recognition is the biometric most suited to the practicalities of travel document issuance, while fingerprinting and/iris available for choice by states for inclusion as complementary biometric technologies (Liersch 2009, p. 96). Having examined the technical aspects and applications of biometrics, it is now time to analyze the theoretical premises of the

"securitization thesis" as evident in the case of migration in tandem with Foucault's concept of "technologies of governance" in today's "surveillance society".

Chapter 2

Theorizing biometrics: Securitization and "Technologies of Governance"

The talk about globalization and the disappearance of space notwithstanding borders in their geographical, spatial and virtual forms has become increasingly central to the debate about the management of migratory flows through the deployment of biometric technologies (Zureik & Satler 2005, p.1). In line with this tendency, discourses have started increasingly to explore and emphasize the destabilizing effects of migration in the political, economic and social realm by identifying migratory flows as a security threat. It was in the wake of 9/11 and the subsequent "war on terror" that a broadening of the global security agenda was achieved not only by catapulting terrorism at the top of the agenda but also making the control of the free movement of people a security priority (Huysmans 2006, p. 19). Indeed, concerns over the passages of people, goods and information across borders have come to dominate the international security agenda leading to the development of a security/migration nexus (Zureik & Satler 2005, p. 1). In this context, the management of migratory flows is now part of a security continuum that facilitates the transferring of security concerns from terrorism, the fight against organized crime and border controls to the free movement of immigrants and asylum seekers (Huysmans 2006, p. 4; Bigo 1994, 1996). Analyses of migration and asylum policy largely reaffirm this intensified securitization of migratory flows as manifested in the strict migration policies later adopted while they underline the increasing political demand for intensifying control of the cross-border movement of people (e.g. Blake, 2003; den Boer and Monar, 2002; Brouwer et al., 2003; Buonfino, 2004; Guild, 2003; Newland et al. 2002; Pickering, 2004; Rudolph, 2006; Welch and Schuster, 2005; Zard, 2002).

In response to these heightened political demands for further control over population movements, we have recently witnessed the development and application of sophisticated technologies that not only ensure the more effective management of migratory flows but they also contribute to the creation of a "surveillance society" (Huysmans 2006, p. 95). More specifically, biometric technologies are increasingly been considered as "technologies of governance" deployed to survey and regulate population movements while rendering the body a source of contestation. To that extent, heightened concerns surrounding borders and mobility have prompted an increased securitization of migratory

flows and have decisively contributed to the spread of biometric identification systems to encompass entire populations (Wilson 2006, p. 89; Bigo 2o02; Lyon 2004). Having said that, it is important to examine the "securitization thesis" as developed by the Copenhagen School of security studies in order to better illustrate how the securitization of migration has in recent years legitimized the development and implementation of biometrical applications often conceptualized in Foucault's notion "technologies of governance".

2.1 The Securitization Discourse

As far as the process of securitization is concerned, security is related to freedom from threat, thus, whatever constitutes a threat is, de facto, a security issue (Buzan et al. 1998, p. 7). In the framework of non-traditional security threats such as migratory flows, however, security has come to be understood as an act that takes politics beyond the established rules of the game and frames the issue-threat either as a special kind of politics or above politics (Buzan et al. 1998, p. 25). In theory, any public issue can be located on the spectrum ranging from *non politicized* (meaning the state does not deal with it and it is not in another way made an issue of public debate and decision) through *politicized* (meaning the issue is part of public policy, requiring government decision and resource allocations) to *securitized* (meaning the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure) (Buzan et al. 1998, p. 24). This process of securitization can therefore be seen as a more extreme version of politicization where an issue is presented as an existential threat and calls for emergent measures to be taken (Leonard 2007, p. 8). Hence, security is a self-referential practice because it is in this practice that the issue becomes a security issue. Not necessarily because a real existential threat exists but because the issue is presented as such a threat (Waever, 1998, 2003, p. 10).

However, it is important to underline that the process of presenting an issue as an existential threat to a referent object does not by itself create securitization- this is a *securitizing move,* but the issue is securitized only if the audience accepts that (Buzan 1991, p. 112). More specifically, a securitization process involves three types of unit: 1) *Referent objects:* things that are seen to existentially threatened and that have a legitimate claim to survival; 2) *Securitizing actors:* actors who securitize issues by declaring a referent object existentially threatened; 3) *Functional actors:* actors who affect the dynamics of a sector and significantly influences decisions in the field of security (Buzan et al. 1998 in Van Dijk

2006, p. 5). These units interact through the exercise of *speech act* which refers to the process through which the *securitizing actor* – some group, movement, party or elite- uses a specific language that is also recognizable by the audience in order to frame an issue as a security threat (Buzan et al. 1998, p. 26). Speech acts do not simply convey information about existing security situations, but they are acts in themselves: saying something is doing something (McDonald 2007, p. 14). Consequently, the world "security" is the act, pronounced by actors in order to produce hierarchical conditions in which security issues are dramatized and presented as supreme priorities of the state or the actor in question (Waever et al. 1993, p. 55). It is evident then that existential threats have to be argued and gain enough resonance to form a platform from which it is possible to legitimize emergency measures that would not have been possible had the discourse not taken the form of existential threats. In this context, the invocation of security is the key to legitimizing the right to use whatever means necessary to handle these existential threats (Buzan et al. 1998, p. 23).

Hence, a successful securitization is based on specific rhetorical structures where an issue is dramatized and presented as an issue of supreme priority in order to justify the need for the deployment of extraordinary means. It is evident then that the securitization discourse refers to the processes of constructing a shared understanding of what is to be considered as a security threat and what the collective response should be (Waever 2003, p. 32). Building upon the premises of social constructivism theory, securitization is then inter-subjectively and socially constructed and consists of three main components: existential threats, emergency action, extraordinary measures (Buzan et al.1998, pp. 203-204 in Mäkinen 2005, p. 10). To this extent, securitization is a part of a discursive, socially constituted, inter-subjective realm (Huysmans 1996). Having analyzed the main premises of the securitization discourse, in the next paragraph I will more closely examine these theoretical premises in migration management in order to better illustrate how the increasing depiction of migration as a security threat justifies the deployment of Foucault's "technologies of governance".

2.2 Securitization of Migration

In recent years, the nexus between migration and asylum policy on the one hand and security concerns on the other hand has become prominent as questions of migration and mobility are increasingly interpreted as problems of security (Brouwer et al. 2003;den Boer and Monar 2002; Guild 2003; Huysmans & Buonfino2008; Bigo 2002, p. 2). An increasing tendency towards the securitization of migration has made immigrants, refugees and asylum seekers both an index of societal fear and a vehicle for inscribing fear as a political instrument for the justification of extraordinary measures to control migratory flows (Aas 2007, p, 38).

Indeed, migration has been increasingly seen as an existential threat and it has done so in two interrelated ways: (1) migration is transfigured into events and developments that existentially endanger the independent identity and functional autonomy of a political unit; (2) in endangering the community it asserts and re-iterates the very existence of the community a as an autonomous political unity Huysmans 2006, p. 51). Securitizing immigration and refugee flows thus produces and reproduces a political community of insecurity where migration is seen as an existential threat (Huysmans 2006, p. 51). For instance, by representing immigration and asylum application as a creeping danger closely related to terrorism and crime, national unity and political support for the deployment of "extraordinary measures" are ensured. Security therefore works on the basis of "insecuring" or in other words, security and insecurity are not opposites but two sides of the security framing coin (Cambell 1992; Waever 1995, p. 56). But what are the reasons behind the securitization of migration? How the politics of insecurity contribute to the deployment of extraordinary measures against the existential threat of migration? In order to answer these questions we need to analyze the reasons behind the securitization of migration as well as the implications of the security/migration nexus in the development and use of biometric technologies in the management of migration.

A first approach to the security-migration nexus reveals that all states have a basic interest or hidden motivations in securitizing migration issues for two main reasons: a) it provides an opportunity for consolidating categories of collective identification and helps mobilize support for the relevant political community, generating greater loyalty through the definition of a common threat (Bigo 2002, p. 65; Huysmans 2000, p. 757) and b) it legitimizes the state in its attempt to introduce more restrictive policies by linking

migration and terrorism as security threats (Buzan et al. 1998, p. 24-25). As far as the former aspect of the security discourse is concerned, it is argued that governments try to present, identify or even "construct" migration as an existential security threat in order to justify actions outside the normal bounds of political procedure in the name of national security stimulating at the same time social allegiance. (Saux 2007, p. 58; Waever 1993 2006, p. 335). It is evident then that securitization of migration constructs political trust, loyalty and identity through the distribution of fear deriving from the depiction of migration as a security threat (McSweeney 1999, p. 48). As the depiction of migration as an existential security threat justifies actions outside the realm of low politics and generates social adherence, the deployment of new technologies as a response to this threat is increasingly becoming the dominant rule in migration management policies (Dillon 2007, p. 18).

It is in this context then that the introduction of biometric technologies in migration management has found its legitimacy in the international realm. Indeed, biometric systems are discursively constructed as a technological buttress preserving community values against perceived external and "alien" threats (Wilson 2007, p. 99, Muller 2004 in Zureik & Satler, p. 91). Within a generalized climate of fear and insecurity deriving from the securitization of migration, an anxious public eager for reassurance has been willing to accept the efficacy of technological innovations such as that of biometrics in migration management (Lyon 2003, p. 85).

As far as the second aspect of the securitization thesis is concerned, many authors have argued that the 9/11 terrorist attacks provided an opportunity for the governments to correlate migration with terrorism, thereby legitimizing the adoption of more stringent migration control practices (Luetdke and Hampshire in Givens et al. 2009, p. 113). More specifically, the security framing of migration and the search for strengthening anti-terrorism policies became closely interrelated as assumptions linking terrorists and immigrants came to dominate the political agenda (Stivachtis 2008, p. 12). In this case, the driving existential question was not the threat that immigrants pose but the free movement of terrorists (Huysmans 2006, p. 64). This politics of insecurity is then a contest of the legitimacy of using particular kind of security knowledge and technologies in migration policy. (Huysmans 2006, p. 53). Hence, this linkage of migration with the anti-terrorist measures adopted as a response to the 9/11 terrorist attacks reveal that the politics of fear as formulated from this inexorable linkage, play an important role in the introduction and legitimization of new technologies of migratory control (Bigo & Tsoukala 2006, p 65). To

this extent, the concepts of biometric border and immigrant biometrics find meaning, as the turn to digital technologies have come to dominate the politics of border management (Amoore 2006, p. 343).

From this follows that the securitization of migration has led to the adoption of restrictive migration measures in an effort to police and monitor mobile population flows (Zureik & Satler 2005, p. 2). Underlying this tendency lays a strong assumption that states have an interest in maximizing societal control by establishing new forms of regulation and surveillance as part of a more restrictive approach to migration issues (Boswell in Givens et al. 2009, p. 25). The securitization thesis, thus, finds its inspiration in Foucaultian concepts of biopolitics and panopticism: the notion that the modern state seeks to increase control through expanding knowledge and surveillance of the populations they seek to govern (Huysmans 2006; Broeders 2007). Indeed, a recent shift in the mode of governmental policing of migratory flows from examination of travelers to the surveillance of the general mobile population through the introduction of new technologies is increasingly taking place in the international arena (Satler 2004, p. 76). Therefore, it would be now important to examine Foucault's concept of "technologies of governance" as part of a modern surveillance society in order to better illustrate the theoretical underpinnings of the uses of biometrics in migration management.

2.3 "Technologies of Governance" in a Surveillance Society

Once, the word "surveillance" was reserved for highly specific scrutiny of suspects, for police wiretapping or for foreign intelligence. More recently, however, surveillance- the gathering of personal data for detailed analysis- occurs routinely, locally and globally as an unavoidable feature of everyday life in contemporary societies (Lyon 2003, p. 87; Muller 2004 in Zureik & Satler 2004, p. 89). In a post-9/11 security drive, a previously absent urgency to surveillance appears to be picked up internationally as biometric technologies are decisively been seen as the "solution" to security threats deriving from migratory flows. (Lyon 2004 in Zureik & Salter, p. 71). In fact, computerization and digitalization are making their mark on surveillance as the latter is turning decisively to the body as a document for identification and as a source of prediction (Lyon 2001, p. 72; Broeders 2007, p. 76; Graham &Wood 2003, p. 228). From Lyon's claims of surveillance as a process of "social sorting" to Haggerty and Ericson' view of surveillance oriented around the idea of

"risk" and "risk management" to Bigo's "banocpticon" and Clarke's "dataveillance", surveillance is becoming a buzz word in the debate about biometrics in migration management (Lyon 2003; Haggerty & Ericson 2000; Bigo 2002;Clarke 1994). Indeed, there is a salient consensus among scholars that the successful monopolization of the legitimate means of movement in tandem with the creation of elaborate technologies and bureaucracies had gradually lead to the computerization of surveillance in migration management (Lyon 2003, p. 68; Boeders & Engebersen 2007, p.1595).

Key to understanding the meaning of surveillance (Staples 1997) or surveillance society (Lyon 2001) lies in the underlying assumption of the surveillance approach. The risks such as those deriving from migratory flows come from beyond the nation state's borders and thus cannot be addressed by traditional state methods of controlling and policing (Lewis in Zureik & Satler, p. 105). On that account, surveillance is frequently, but not exclusively, carried out using centralized networked technologies which vastly increase its capacities and scope and offer possibilities of successful management and monitoring of mobility flows on the international level (Lyon 2001, p. 29). Central to this is the recent debate on the use of biometric technologies in the management of migratory flows. More specifically, in examining the object of surveillance, many academics highlight the significance of biometrics - the conversion of the body into data- in the formation of a surveillance society (Zureik 2004;Muller 2004). While some scholars argue that the politics of biometrics formulate the contemporary politics of security and identity, others conceive biometrics as the byproducts of a politically constructed "fear economy"(Lewis in Zureik & Satler 2004, p. 84; Wilson 2006, p. 89). Regardless of the current academic debate on biometrics, there is a general consent that surveillance of mobile populations through the introduction of biometric technologies is becoming the rule in migration policies (Van der Ploeg 2007, p. 5).

Hence, in this "network society" (Castell 1996), Foucault's "technologies of governance" consist an important theoretical concept to understand the role and implications of biometric technologies in migration policies and is therefore an important point of departure in this theoretical analysis. The notion of "technologies of governance" is based on Foucault's concept of "governmentality", a concept that offers a new understanding of the power of techniques and strategies through which a society is rendered governable (Foucault 1991in Burchell, p. 90; Jones 2007, p. 17). More specifically, Foucault argues for a concept of power that is not based on a hierarchical, top-down power of the state. Instead he widens our understanding of power to also include the forms of

social control in disciplinary institutions such as schools, hospitals and psychiatric institutions (Foucault 1991 in Burchell, p. 92). This form of power applies itself to immediate everyday life that categorizes the individual, marks him by his own individuality, attaches him to his own identity, imposes a law of truth on him which he must recognize and which others have to recognize in him (Foucault 2000a, p. 328). It is a form of power that makes individuals subjects and establishes more efficient forms of social control (Foucault 2000a, p. 328). There are two meanings of the word "subject": subject to someone else by control and dependence; and tied to his own identity by a conscience or self-knowledge. Both meanings suggest a form of power that subjugates and makes subject to (Foucault 2000a, p. 340). From Foucault's point of view, governmentality can be seen as an "art of government" that is not limited to state political power alone, but one that includes a wide range of control techniques, and that applies to a wide variety of objects, from one's control of the self to the "biopolitical" control of populations (Foucault 2000b, p. 410).

Having said that, Foucault's notion of *biopower* as a technology of power, as a way of managing people as a group, is also rather significant in understanding the introduction of biometrics in migration managaement. What is critical in understanding the notion of biopower is the fact that the distinctive quality of this political technology is that it allows for the control of entire population (Foucault 2000b, p. 406). Biopower is literally having power over other bodies, "an explosion of numerous and diverse techniques for achieving the subjugations of bodies and the control of populations" (Foucault 2000a, p. 365). It relates to the government's concern of fostering the life of the population, and centers on the poles of discipline ("an anatomo-politics of the human body") and regulatory controls ("a biopolitics of the population") (Foucault 2000b, p. 410). To sum up, Foucault argues that "we must distinguish the relationships of power as strategic games between liberties – strategic games that result in the fact that some people try to determine the conduct of others – and the states of domination, which are what we ordinarily call power. And, between the two, between the games of power and the states of domination, you have technologies of governance" (Foucault 1988, p. 19).

Both notions of "technologies of governance" and biopower refer to "micro techniques of discipline that target and treat the body as an object to be watched, assessed and even manipulated (Foucault 1997, p. xi). It is clear then that these techniques of governance rely heavily on sophisticated computer technology and complex mathematical modeling to mine data and single out "suspects" (Amoore & De Goede 2005, p.151). One of the most interesting aspects of Foucault's approach is that it unpacks specific

technological devices (i.e. statistical technologies of monitoring) of the exercise of governmental power in the context of analysis of the particular rationalities or matrixes of government that they articulate and by which they are traversed (Foucault 2004). In rejecting various essentialist, transhistorical, universal, and deductive analyses of the state and state power, Foucault created a space for exploring its "polymorphous crystallization" in and through interrelated changes in technologies of power, objects of governance, governmental projects, and modes of political calculation. Indeed, he argues that ''the state is nothing more than the mobile effect of a regime of multiple governmentalities based on the use of technologies of power that seek to discipline the individual body or to regulate population processes" (Foucault, 2004: 79).

Based on these theoretical premises, biometric technologies are perhaps then best understood as techniques that govern both the mobility and enclosure of bodies (Amoore 2006, p. 342). In line with Foucault's concept of "technologies of governance", many scholars have treated biometrics as automated and asocial technologies of control (Pickering & Weber 2006, p. 9). As already indicated, governance involves the use of knowledge such as technical, social, administrative in an effort to manage population groups through identification, categorization (inclusion and exclusion), and a monitoring process in order to address the precautionary risks such as those deriving from migratory flows (Zureik & Hindle 2004, p. 174). The introduction of biometrics can thus be seen as an attempt to mobilize discourses of vigilance, prevention and monitoring to govern uncertainty, or "govern the ungovernable" as in the case of migration (Muller 2008, p. 206). It is clear then that the free movement of people is not simply managed through a territorial technique that externalizes the excess such as border control but also through a "biopolitical technique" that internalizes the excess in the population such as the databases and surveillance of movement (Huysmans 2006, p. 93). In fact, the management of border has ceased to be a matter purely of geopolitical policing and discipline, in the sense of governing the entry and exit of peoples across mapped space, and has became a matter of "biopolitical management" (Walters 2002, p. 562) Hence, the development and application of technological devices such as European visa and databases structure the relation between security and migration and emerge as key regulatory mechanisms of migratory flows (Staples 1997, p. 25; Bigo, 2002, p. 67; Ceyhan and Tsoukala, 2002).

2.4 Conclusion

To conclude then, in the aftermath of the 9/11 attacks and the subsequent "globalization of fear and insecurity", high-tech solutions to problems of security have come to dominate the political debate (Van der Ploeg 2003; Zuriek & Hindle 2004; Davis 2001). This is mostly evident in the proliferation of biometric technologies in migration management as the securitization of migration has lead to the legitimization of the deployment of "extraordinary" security measures in the international arena (Buzan et al. 1998; Wilson 2006, p. 88). As international actors attempt to maximize societal control over migratory flows by establishing new forms of regulation and surveillance, the reach of biometric identification is expanding to encompass whole mobile populations contributing to the establishment of a "digital rule" (Wilson 2006, p. 90). It is clear that we are witnessing a significant turn to scientific and managerial techniques in governing the mobility of bodies as the extension of biopower such that of the body, in effect, becomes the carrier of the border (Amoore 2006, p. 348). This is true in the case of the EU that is currently laying the foundations for an impressive digital infrastructure aimed at securitizing EU migration policies (Broeders 2007, p. 88). Apart of an attempt to ensure efficient control over mobile populations, international actors such as the EU move on to establish "a coherent approach on biometric identifiers or biometric data for documents for third-country nationals, EU passports and information systems" (European Council 2003). EU's digital infrastructure is therefore increasingly expanding not only through the introduction of biometrics in EU passports and identities but also through the development of computerized information systems such as the Schengen Information System and the Eurodac database (Broeders 2007, p. 71). Having said that, it is now important to examine these developments in the EU through the prism of the securitization thesis and Foucault's "technologies of governance".

Chapter 3

EU Digital Borders and E-Passports: Expanding Surveillance?

Both the "securitization discourse" and the notion of "technologies of governance" introduce an analytical framework that help to comprehend how the use of knowledge (technical, social, administrative) is seen to contribute to the better management of population movements through identification, categorization (inclusion and exclusion), monitoring and social controlling (Foucault 1997, p. 193-212). Indeed, these theoretical premises are of explanatory validity in the case of EU's digital borders where a centralized approach to enhanced surveillance has gradually come to dominate its modus operandi in migration policies. To this extent, the development of European databases such as the Schengen Information System, Eurodac and Visa Information System- and the introduction of biometrics in EU citizens' passports are seen as the key technological initiatives developed to ensure the efficient control of migratory flows into and within the EU. It is evident that the EU is increasingly adopting a centralized surveillance approach that is based on intensive internal migration controls and electronic surveillance in an attempt to better address the heightened security concerns deriving from population mobility (Huysmans 2006, p. 98; Lewis in Zureik & Satler 2005, p. 106)

Based on these assumptions, we will start-off to examine the actual developments with regard to "datasurveillance and border control" in the European Union. More specifically, this chapter examines the introduction of biometric applications in passports of EU citizens and analyses the actual use and content of SIS and its second generation SIS (SISII), and other EU databases such as Eurodac and the Visa Information System. After analysing these developments, this chapter will conclude by arguing that the technical, political, and legal choices related to for the development of an EU digital rule in migration management, which are now being made at the EU level, will increasingly bring to light questions regarding privacy rights and civil liberties concerns. To that extent, EU's legitimacy in deploying "extraordinary" technological measures for the secure management of people's mobility could be utterly challenged by those arguing that EU's progressive digitalization could lead to group differentiation and social sorting in the name of security.

3.1 EU Migration Policies: In the path of "Securitization and Digitalization"

Before examining the recent "securitization and technologization" of EU's immigration policies, one should first understand that there are currently two trends taking place in the field of migration in the EU. On the one hand, real structural factors of managing flows of people are linked with the transformations of the possibility to travel and with the development of individuals' increasing desire and imperative to move. On the other hand, they are determined by technologies of identification, the policing at distance and the collaboration between the different internal agencies on global level attempting to control more efficiently how and where people move to (Bigo in Guild & Bigo 2005, p. 50). To that extent, the increasing deployment of practices and technologies associated with verifying the identity of persons has become one of the main preoccupations of EU's member states (Toprey 2000). Indeed, the need for the adoption of more sophisticated devices and technologies of border control and surveillance such as the introduction of biometric techniques in travel documents and the development of centralized migratory databases in the EU, is at the centre of the EU's biometric debate (Ashbourn 2005, p. 15). In the light of these developments, one question needs to be answered: which factors have contributed, facilitated and even legitimized this increasing digitalization of EU's immigration policies?

Partly, has the renewed emphasis on biometric techniques in the aftermath of 9/11 and the subsequent "war on terror" lead to an intensified interest in the development of centralized identification databases and technologies in migration management policies. (Ceyhan in Guild & Bigo 2005,p.78). To that extent has biometric identification played a significant role in the development of EU migration policies where distinct initiatives were launched with regards to EU citizens and towards third country nationals (Laboratore 2007, p. 115). More specifically has the EU increasingly attempted to develop and adopt new technologies of identification in order to securitize identities and identification means while monitoring the movement of people inside a given region as well as across borders (Ceyhan 2008, p. 114). The development of a brand new market of technologies of identification has lead to the hyper - technologization of EU migration policies where the "securitization" of certain groups such as migrants and asylum seekers justify the extensive use of these technologies beyond the reach of terrorism or criminal activities (Bigo in Guild & Bigo 2005, p. 78-9).

Indeed, these technologies such as biometrics have recently become the key element of new EU policies aimed at increasing safety, interoperability, availability and efficient border control. More specifically, EU member states have embarked in a course of transforming immigration from a national and political question into a transnational and "technological" one, by presenting migratory flows as a matter of security technology (Bigo in p. 81; Bigo 1996). The recent transformation of the notion of frontier within the discussion between internal and external frontiers of the European Union, in tandem with the "construction" of migration as a security threat, has facilitated the linkage of freedom of movement and policing and thus the act of policing in the name of freedom (Bigo in Guild & Bigo 2005, p. 51). In the European context, especially from the main narrative of the four freedoms of the EC market that includes the freedom of movement of people, the relationship between border controls and immigration laws on the one side, and politics and social practices of control on the other, is rendering EU's migration policies a complex case. Indeed, in both Europe and the US, framing the link between frontiers and control is constantly constructed as a security issue: as a well-balanced organization between freedom of movement and necessary measures of protection from migratory flows (Bigo in Guild & Bigo 2005, p. 51). Hence, the term "border security" has become a common usage in EU policy. It is indicative of a linkage between security concerns and migratory flows.

Central to the academic debate is the idea that the European Union is in a confused attempt to find a post-national, post-state form of governmentality where a trasnationalization of the technological systems of control corresponds or even anticipates the transnational migratory flows (Bigo in Guild & Bigo 2005, p. 51). To this extent, it is of no surprise that the European Union has over the years attempted to address the security concerns deriving from migratory flows by resorting to new techniques based on dissuasion, control and surveillance (Bigo in Guild & Bigo 2005, p. 78). This is mostly evident in EU's counter terrorism strategy that is trying to increase border security by widening the range of information available to the police and authorities responsible for internal security on persons who move or seek to move across borders (Baldaccini 2008, p. 48). Indeed, in most instances cross-border mobility comes at the cost of providing personal information to the authorities and it is increasingly fingerprints and facial biometric data that are now captured in visa, passports, residence permits and identity cards. Central repositories of this information, such as the Schengen Information System, Visa Information System and Eurodac, are to be interlinked and opened up to police

searches with the purpose of controlling immigration and safeguarding security. The next section will offer an overview of the development of EU's E-passports that consist the advanced versions of a combined national identity card and traveling document which holds digitized biometric features of its associated individual for enhanced security of personal authentication (Abid & Afifi 2008, p. 99).

3.2 "Document Security": Biometric features in EU's E-passports

The concept of "document security" merges the separated yet indivisibly policies on border control and internal security and captures vividly the emphasis on the enforcement aspects of the EU immigration policies. To that extent, this policy relies on the ever-greater sophistication of security technology and in particular the use of biometric features in passports, visas and identity documents (Baldacini 2008, p. 32). Indeed, the inseparability of illegal immigration, organized crime and border issues was confirmed when the EU agreed to ensure coordination between migration policy and external relation's instruments. The evidence so far has been that terrorists tend to cross borders legally, use their real identities and reside legitimately in the host country (Lodge 2004, p. 263). For instance, those who were involved in the US attacks and in the Madrid bombings had valid or expired visas or were equipped with legitimate identification cards. Nevertheless, member states see the detection of persons who attempt to enter the EU on forged document and the prevention of the use of false identities as essential for the EU's security. In that context, the most reliable means of detecting counterfeit of forged documents and ascertaining whether the holder of a document and the person to whom the document has been issued are one and the same is the in the use of biometrics (Baldacini 2008, p. 33).

To that extent, the 1999 Tampere European Council underscored the importance of the borders for strategies to combat cross-border crime and illegal immigration (European Council 2004). Simultaneously, a raft of measures followed secret US-EU meetings on managing migration, information exchange, stolen passports and blank passports, the creation of a database, and measures (Abid & Afifi 2009, p. 338). By October 2000, member governments had agreed to introduce minimum security standards for the production and issue of new travel documents by 2005 (passports) and 2006 (identity cards and short-term passports). In September 2003, the European Commission produced

two draft Regulations to introduce two sets of biometrics data (fingerprints and digitized photographs) on passports, visas and residence permits for third country nationals by 2006 (European Commission 2006). However, a number of member states wanted further biometric data to be stored and the June 2003 European Council of Thessaloniki invited the Commission to prepare proposals for a "coherent approach" in the EU on biometric identifiers to result in "harmonized solutions for documents for third country nationals, EU citizens' passports and information systems" (European Council 2003).

The year 2004 was a very intense period with regard to finalization of biometric identification policies; this was partly linked to the revamped emphasis on fighting terrorism following the attacks of 11 March in Madrid (Liberatore 2005, p.10). In October 2004 the Interior Ministers of five EU countries- France, Germany, Italy, Spain, UK- met in an "informal meeting" in Florence and agreed on the need to include biometric identifiers, both fingerprints and facial image in passports (Liberatore 2005, p. 10). Such proposal was later debated where additional countries supported it (Poland, Slovenia, Malta, Lithuania,) while others (Sweden, Finland, Estonia, Latvia) opposed the introduction of fingerprints as mandatory and two countries (Denmark, Portugal) did not oppose but raised the issue of costs. On 4-5 November 2004 the Hague Programme adopted by the European Council recalled the importance of adopting biometric identifiers; interestingly the topic of "biometrics and information system" came under the heading of "strengthening freedom" (European Council 2004a, p. 25) A Regulation on standards for security features and biometrics in passports and travel documents in the EU was adopted in on the 13 December 2004 (European Council 2004b). This Regulation that was prompted by American demands for the inclusion of high-security features in the passports of countries subject to the American visa waiver programme (VWP), provides for the inclusion of facial image and fingerprints in interoperable formats, for the rights to verify and ask for verification of data (Salter 2004, p. 73). As far as the time framework for the implementation of these biometrics in passports and travel documents is concerned, the Regulation requires passports to be issued with facial image chips by August 2006 and digital fingerprints to be integrated by 29 of June 2009.

The Community competence to adopt this Regulation on standards for security features and biometrics in passports and travel documents in the EU has been questioned, given that the power to adopt legislation to facilitate the free movement rights of EU citizens explicitly excludes provisions on passports, along with provisions on identity cards and other documents concerning EU citizens (De Hert 2005). More specifically,

while the passport Regulation is based on the EC competence to enact measures dealing with the crossing of external borders passports are also frequently used within the EU's territory as a proof of identity and the legislation would arguably have required a specific legal basis in this respect too (Spokkereef 2008, p.279). It is important to notice that the recently empowered Lisbon Strategy amends the EC Treaty so as to place the adoption of measures on passports, identity cards and similar documents in the relevant Title IV Chapter on border checks. This seems to be an implicit recognition of the shaky legal position in the competence exercised so far (Spokkereef 2008, p.281).

More recently and specifically in February 2008, the European Commission presented a new "Border Package" setting out its vision of how to foster the further management of the EU's external borders (Guild et al. 2008, p. 1). Billed in a Commission press release as a "comprehensive vision for an integrated European border management system for the 21st century", one of the key elements of this package is a Communication aimed at establishing a EU entry/exit system registering the movement of specific categories of travelers at the external borders of the EU. What is critical in understanding the significance of this package for the case of EU passports is the fact that this Communication recommends the setting up of an Automated Border Control System enabling the automated verification of a traveler's identity (for both citizens and non-EU citizens alike), based on biometric technology as well as an Electronic Travel Authorisation System – abbreviated to ETA4 – which would oblige EU and non-EU travelers to provide personal data for a pre-departure online check (Guild et al. 2008, p. 3).These security tools and techniques imply the systematic checking of everyone entering and leaving the EU for at least three categories of persons: a) third country nationals who have visas containing biometric data, which will be checked at the border; b) third country nationals who do not need visas for a short stay in the EU whose biometric data will be taken at the border and most importantly c) citizens of the EU whose biometric data will be incorporated into their passports which will be swiped on entry and exit (Guild et al. 2008, p. 5). In the context of this "Border Package", the Commission also proposes the establishment of a EU Passenger Name Record (PNR) System, mimicking the EU-US PNR Agreement of July 2007. This proposal is expected to create the same sort of public relations problems as do similar US measures among a traveling public that finds itself increasingly the object of state suspicion, with no concrete reasons or grounds (Guild et al. 208, p. 4). Indeed, this plan raises several

important questions: Is it feasible and necessary? Does it have a legitimate objective? Is it consistent with EU data protection rules, fundamental rights and the principle of proportionality? Is there any appreciable added value of such a system, bearing in mind its high costs? Which are the factors that facilitated and later legitimized the introduction of biometrics in EU citizens' passports?

It is evident that requirements for greater security in the European Union (EU) that have lead to the development of biometric passports, are driven not only by internal concerns that link inexorable security threats and migration but also by external factors. More specifically, the United States has played an instrumental role in leading and setting the final standards for the global introduction of biometric passports (American Civil Liberties Union 2004). For instance, the US Visitor and Immigrant Status Indicator Technology programme (US VISIT) of border controls that collects biographic, biometric, travel and biometric identification of non-US nationals at the point of entry to assist border guards to verify the individual's identity on arrival and departure consists an example of US efforts to globalize the use of biometrics in travel documents (Amoore 2006, p. 338; Amoore & De Goede 2005, p. 166; Redpath 2007, p. 30).

Before examining the EU's informational databases in the framework of migration management, it is important to notice that the deployment of an e-Passport in the EU has proven to be a rather controversial issue. There are many reasons for this controversy, but the most prominent one concerns the possible social implications deriving from the introduction of biometrics in passports. More specifically, the collection and later provision of biometric data is seen as an invasion of personal freedom as for many people, fingerprint identification, for example, is perceived to be too closely associated with criminality, while others report legal implications for the provision of free movement of people (Kruelle et al. 2005, p. 537). Furthermore, "invasion of privacy" fears and personal security concerns exist over where and how the biometric information will be stored and who will have access to it (Liu 2008, p. 50). In parallel with these rising concerns over the introduction of biometrics in travel documents, the increasing expansion of the EU's Information networks through the development of several databases have come to intensify these concerns and reveal the development of a centralized surveillance approach in EU's migration management.

3.3 Expanding the European Information Network: SIS, Eurodac,VIS

Regardless of the "securitization" of travel documents, the EU's strategy on migration issues is increasingly focusing on the development of schemes that retain and process data on individuals. In a general framework, irregular migrants have three possible "migration histories". They either crossed the border illegally (with or without help), they were asylum seekers and stayed after the claim was rejected, or they came on a legal visa and stayed after its validity expired (Broeders & Engbersen 2007, p. 1603). The network of databases develops accordingly. Irregular migration itself defies registration, but irregular migrants found in member states can be registered in the SIS. Those who enter though asylum procedures will be registered in Eurodac and those who enter a legal visa will, in the future, be registered by VIS (Broeders 2007, p. 85).

It is evident that the Eurodac, the VIS, the SIS, illustrate the range of tasks of information exchange that can be achieved in the framework of EU's immigration initiatives. Since the Treaty of Amsterdam, political attention for irregular migration became more structural and gradually took on a grim tone: policy on irregular migration became "the fight against illegal migration" (Broeders 2007, p. 77). To that extent, EU member states developed a network of immigration databases at the EU level aimed at documenting these immigration histories in order to "re-identify" illegal aliens found on the territories of the member states (Broeders 2007; Engbersen & Broeders 2007, p. 1603). More specifically, the development by the EU of these large-scale electronic surveillance systems are seen as instruments for border controls as well as for internal migration surveillance (Broeders in Fassman et al. 2009, p. 250). As the active surveillance of irregular migrants depends heavily on information and knowledge production, EU member states cooperate and contribute to the development of this EU's digital infrastructure. In other words, control depends on information to make society, in the words of James Scott "legible" so that the state and in our case the EU can act and implement policy (Scott 1998 in Broeders 2007, p. 73). In the current information age where filing cabinets are rapidly replaced with searchable databases and where technology simplifies interconnectivity and (remote) accessibility, computerization and technological innovations play a leading role in matters of migration management

(Broeders 2007, p. 74). Finally, what is critical in understanding the significance of these databases is the fact that they all contain personal data on third-country nationals and are being developed, expanded in scope and equipped with the latest security technology with a view to their potential use in fighting crime and preventing security risks. Hence, the political and symbolic attributes of securitization instruments such as the EU's databases suggest that the EU's counter-terrorism strategy transforms the schemes of information exchange into securitizing tools of migratory flows (Balzacq 2008, p. 85).

3.3.1 Schengen Information System (SIS) and SIS II

The Schengen Agreement which was originally negotiated outside the normal EU institutions, aimed at giving real meaning to the long-standing European goal of free movement by abolishing the internal borders among the signatory states (Broeders 2007, p. 77). In fact, the Schengen Agreement including the Schengen Information System (SIS)- it's "dataflagship"- were integrated into the EU through the Treaty of Amsterdam in an effort to strengthen EU's borders by preventing irregular migration (Dhian Ho 2004, p. 3). More specifically, "Schengen" operates two comprehensive registration and surveillance systems. The first is the Schengen Information System (SIS), a data-based registration and surveillance system and its intended uses concern national security, border control and law enforcement purposes (Guild 2008, p. 4). The SIS is in operation and is considered as a secure governmental database used by several European countries to maintain and distribute information on individuals and pieces of property of interest (Guild 2008, p. 4). The second system, SIRENE, which stands for Supplementary Information Request at the National Entry, is twinned with the SIS as an auxiliary or supplement system (Broeders in Fassmann 2009, p. 257).

The SIS is made up of a central database (called C-SIS) that is physically housed in a heavily guarded bunker in Strasbourg and of national SIS-bases (called N-SIS) in all of the Schengen states. Its purpose is to maintain "public order and security, including state security, and to apply the provisions of this convention relating to the movement of persons, in the territories of the contracting parties, using information transmitted by the system" (Article 93 of the Schengen Convention). This broadly defined purpose provides the legal base for a large data system that stores information on persons and objects. Not all authorities have overall access to the system; immigration authorities for example only

have access to the data on irregular migrants (Brouwe 2008, p. 12-13). The system is a so-called hit/no hit system: a person is fed into the computer and produces a 'hit' if he or she is listed in the database. Even in the case of a hit, not all information is readily accessible rather, the computer 'replies' with a command, such as apprehend this person' or 'stop this vehicle' (de Hert, 2004: 40).

However, the SIS was not designed for detailed data exchange and in practice it serves as an index to the associated SIRENE system, which facilitates the exchange of complementary information, including fingerprints and photographs (Broeders 2005, p. 157). Although SIRENE is often described as the operational core of Schengen, there is no reference to the system in the Schengen Convention (European Commission, 2000: 19). The factual data are stored on the SIS but the SIRENE system makes it possible to exchange "softer" data such as criminal intelligence information. In order to make this a "convenient" arrangement, the national SIS and the SIRENE bureaus are in most countries entrusted to the same organization, usually a central police department responsible for international cooperation. Though the SIS is an instrument intended in maintaining "order and security", its main preoccupation seems to be with illegal migration (Guild 2001).

Furthermore, SIS has proven to be a rather popular instrument. Indeed, the enlargement of the EU and national wish "lists" of countries such as the UK, Norway, Iceland and Switzerland to participate in the SIS through the conduction of relevant association agreements has lead to the development of a second generation system (De Hert 2004). More specifically, this rapid growth of the Schengen Group has led to the decision for the development of a second generation of the system the so-called SIS II which would accommodate the new members and facilitate new additional functions (de Hert 2004). The SIS II became operational at the end of 2008 and will allow for a wider use and new categories of data, and be up-to-date with the development in information technology (Baldacini 2008, p. 37). What is important to notice is that after the 9/11 attacks, its function extended to provide information in the context of "the fight against terrorism" and adapted to enable the storage of biometric data such as photographs and fingerprints (Baldaccini 2008, p. 37).

A progressive incorporation of biometric technologies to the SIS is one of the key aspects of the current development in the European Information Network. More specifically, the SIS is currently based on alphanumeric data that allow only for two results: hit or no hit. Biometric systems, instead, are designed to search for an acceptable

degree of similarity and are more effective, therefore, in linking information to persons (European Commission 2008). They will also significantly improve the possibilities for police searches. In particular, biometric data can be used both to confirm someone's identity (one-to-one search) and to identify somebody (one-to-many search) (Eliott 2009, p. 1). One-to-many searches transform the nature of the SIS from a database used for control purposes to one which can be used for investigative purposes, enabling so-called "fishing expeditions" in which people registered in the database will form a suspect population (Mitsilegas et al 2007, p. 8).

Many critics, among them data protection authorities, have warned that the use of biometrics as a unique means of identification can have serious consequences for those who are wrongly identified, given the tendency of authorities to overestimate the reliability of biometrics (Andronikou et al. 2008, p. 18). Indeed, the haste in allowing the biometric search function is troubling in the absence of provisions on misused identity and inaccurate information due to technological failure, let alone any provision on compensation for those who have been wrongly identified (Baldaccini 2008, p. 38). Furthermore, there is wide divergence in national practices to registering people in the SIS, and this is likely to remain so with SIS II, as the relevant legislation does not harmonize the substantive rules for listing persons to be denied entry, thus continuing to leave a wide degree of independence to Member States (Lodge 2006). Some Member States, notoriously Germany and Italy, interpret the criteria for listing unwanted third-country nationals rather widely, with the result that they account for the vast majority of data entered into the system (Guirandon 1999, p. 27). This is a matter of considerable concern as once biometric searches are enabled those 750,000 third-country nationals (a number likely to grow considerably with the expansion of the database) will form part of a suspect population whose data will be crawled through for the purpose of police investigations (Deslol 2008, p. 4).

Hence, the EU's securitization agenda is resulting in a shift of purpose of the SIS from a border control tool to a reporting and investigation system for general crime detection purposes. Indeed, the SIS database, originally conceived of as a compensatory measure for the lifting of internal border controls, is being developed in a way that disconnects it from its original purpose of allowing the free movement of people in the Schengen area and makes it an objective in itself (Ho 2004, p. 16). This disconnection is best exemplified in the Council's decision to extend, from 1 September 2007, SIS access to the new Member States that acceded to the EU in 2004 (with the exception of Cyprus) prior to the lifting of checks at internal borders with the Member States concerned (Council Decision 2007). Finally, the SIS II came to be seen as a flexible tool that will be able to adapt to changed

circumstances (CEU 2003, P. 18). In other words, we could witness in the future the proliferation of functions and granted access to new organizations and even the integration of all systems into one European Information System fostering, thus concerns over privacy perils and civil liberties risks (Brouwer 2004, p. 5).

3.3.2 Eurodac

A second important European database is the Eurodac system, which became operational in January 2003. The development of the system was a long and politically bumpy ride and the decision to set up this system was taken in 1991. It was not until 2003 that it came to be realized (Aus 2006). By then, the scope of Eurodac was widened to become a community-wide system for the comparison of fingerprints of asylum claimants by curtailing the possibilities for "asylum shopping"- i.e. individuals entering into the asylum procedure in more than one country successively- and by determining which state is responsible for an asylum claim (Broeders 2007, p. 82). Hence, Eurodac is essentially an immigration database developed to support the implementation of the European asylum policy. More specifically, this computerized system allows for the identification of third-country nationals who may have already lodged asylum applications in the EU and whose data were already enrolled by one Member State (Baldaccini 2008, p. 42). With its establishment, fingerprints of asylum seekers, whether inside or outside the European Union's borders, have been taken and digitally transferred from member states to a central Eurodac unit for comparison against the existing database (Wilson 206, p. 101). Fingerprints of asylum seekers can be stored for up to ten years or immediately erased if an applicant is granted a nationality in a member state. In addition to asylum seekers, Eurodac is also a biometric database of "persons who have crossed an external frontier of the Community in an irregular manner" (Europa 2003). These "foreign nationals" have their biometric data retained for two years or immediately erased if they receive residence permit or leave the territory of the European Union (Wilson 2006, p. 101). Like the SIS system, Eurodac is a hit/no hit system and it is considered to be a rather effective and cheap system (Broeders 2007, p. 83).

As far as the rationale behind the development of this database is concerned, Eurodac was justified by the European Council in terms of the need to accelerate decisions on asylum bids (Wilson 2006, p. 101). More specifically, the establishment of

Eurodac was seen as a response to the perceived need to stem "asylum shopping" across member states and separate those categorized as "legitimate" asylum seekers from other categories of migrants (Lodge 2004, p. 241). However, the Standing Committee of Experts in International Migration, Refugee and Criminal Law has provided some counter-arguments against the wide use of Eurodac information. These arguments refer to the infringement of the principle of the purpose limitation; concerns over the stigmatization of asylum seekers; the risk of proliferation of unreliable information; and the fears of endangering persons in need of protection (Sprokkereef 2008, p. 281). These heightened concerns illustrate how future data protection comes under considerable pressure as a result of the relatively open ended approach to the limitation of the purpose principle. Furthermore, when it comes to collecting and storing biometrics of European citizens and asylum seekers, an extensive legal interpretation of the original purpose for which the data were collected may well lead to a use that was not foreseen by those providing a sample (Spokkereef 2008, p. 281). In view of the fact that many samples will have been given on a non-voluntary basis, and the legal basis for profiling and surveillance differ considerably form country to country, leaving the individual in the dark about what will eventually be done with his or her biometrics (Pap 2008). Hence, concerns over the legal basis and technical functions of Eurodac have proliferated in recent years and have revealed the need for serious consideration and re-evaluation of the Eurodac's role in migration management processes.

As far as the future of this database is concerned, the Commission reports that it "will explore, on the basis of further analysis and full impact assessment, the possibility to extend the scope of Eurodac with a view to use its data for law enforcement purposes" (COM 2007). The issue of police access to Eurodac is, however, well beyond the stage of exploration as member states have already made relevant plans that have been speedily advanced under the German Presidency (Baldacini 2008, p. 44). More specifically, a Presidency paper that sums up the arguments of law enforcement use of Eurodac discussed at the beginning of 2007 argues the following:

> Frequently, asylum-seekers and foreigners who are staying in the EU unlawfully are involved in the preparation of terrorist crimes, as was shown not least in the investigations of the suspects in the Madrid bombings and those of terrorist organization sin Germany and other Member States.

And:

> Access to Eurodac can help provide the police and law enforcement authorities of the Member States with new investigative leads making an essential contribution to preventing or clearing up crimes.
>
> Council Document
> 5291/07, 12 January 2007

It is evident that the increasing depiction of illegal immigrants as criminals and the subsequent securitization of migratory flows provide legitimacy to the Council's initiative to involve police authorities in the use of Eurodac. Although it has been recently stressed out that police access to Eurodac should be subject to strict compliance with the rules governing the protection of personal data, it still remains to be seen what detailed data protection rights will be proposed and to what extent safeguards against inappropriate uses of the database will be ensured. The question that still remains largely unanswered is whether it is acceptable to subject anyone on the Eurodac database to a greater surveillance than others in the population, particularly as the disproportionate criminal activity that might result from this group will in turn foster discrimination and reinforce widespread prejudices (Baldaccini 2008, p. 44).

3.3.3 Visa Information System (VIS)

In the framework of the "fight against illegal immigration", the Visa Information System (VIS) is the next logical step in the emergent network of databases (Broeders 2007, p. 85). More specifically, at the extraordinary Council meeting that followed the 9/11 attacks, the Home Affairs and Justice Ministers decided that procedures for the issue of visas should be tightened and that the Commission should make proposals for the establishment of a network for information exchanges concerning visas issued by member states (European Council 2001). As far its functions are concerned, the VIS is to collect and store fingerprints and other biometric identifiers of all third-country nationals applying for short-term visas (Baldaccini 2008, p. 40). Hence the VIS will make it possible to identify those irregular migrants who legally traveled into the EU at any border (Broeders & Engbersen 2007, p. 1604).

A Council Decision that gives the Commission the mandate to prepare the technical

development of VIS through Community financing was adopted on 8 June 2004 (European Council 2004). In the same year, the Commission proposed implementing legislation defining the functionalities of the information system, and establishing procedures and conditions for the exchange of data between member states on short-stay visa applications. The data to be processed include not only alphanumeric data and photographs but also applicants' fingerprint data. Agreement on this Regulation was reached at the Justice and Home Affairs Council meeting of 12/13 June 2007. Information will be collected by member states' consulates and then transferred to a central database where it will be accessible by all relevant authorities. The system's capacity will provide for the connection of at least 12,000 users in 27 Member States and at 3,500 consular posts (JHA Council 2007). As citizens from 134 countries require visas to enter the EU, it had been possible for an applicant that had been rejected by one country's consulate to continue applying to other consulates (Euroactive 2005). Once the VIS is in place, probably in 2010, this will not be possible. Information on previous applications and reasons for rejection would be available through the new system (JHA Council 2007. The inclusion of fingerprint data is intended to allow the exact verification of somebody's identity. Member States are already planning for the collection of biometric data for the VIS at consular posts, beginning with posts in North Africa and the Near East in line with the Council's view that regions of high risk should be prioritized (Boniface et al. 2008, p. 4).

As far as the objectives of the VIS are concerned, these, as set out in the Council guidelines, concern the following: to combat fraud; improve consular cooperation; facilitate border and police checks; prevent "visa shopping"; facilitate the expulsion of third-country nationals; improve the administration of the common visa policy in order to improve internal security against terrorism and crime (Council Conclusions 2004). Subsequently, the Council expressed the view that "the aim of enhancing internal security and counter-terrorism can only be fully achieved if it is ensured that the member states' authorities responsible for internal security have access to the VIS (Council Conclusions 2005). It is evident that when the VIS is completed, the EU will have a new digital border that will survey the immigrant population rather than the territorial border (Bigo & Guild 2005). The central purpose of the system hence refers to the internal surveillance of irregular migrants and its capacity to detect and identify them on the territory of member states (Broeders 2007, p. 85).

In the meantime, the proposal concerning access to this database by relevant

authorities for law enforcement purposes has also been foreseen. Designated authorities of member states and Europol may access the data kept in the VIS if there are reasonable grounds to consider that consultation of VIS data in a specific case will substantially contribute to the prevention, detection or investigation of terrorist and other serious criminal offences (European council 2007). Police access to the VIS is far from insignificant. VIS is an information system developed in view of the implementation of the European visa policy. It is not a law enforcement tool (European Data Protection Supervison 2007, p. 3). As mentioned above, it will be able to contain the data concerning about 20 million visa applicants annually and, according to Commission estimates, 70 million fingerprint data will be stored in the system in the first five years of its operation. Routine access to police would entail a disproportionate intrusion in the privacy of travelers (Sprokkereef 2008, p. 281). While under the legislation conditions of access are restricted to specific cases and subject to a case-by-case examination of the necessity of such access, there is concern that the provisions leave room to a broad interpretation which might in practice lead to police access being routinely granted (Mitsilegas 2007, p. 392). In the light of this risk, the data protection authorities advised that police access to the VIS should be made subject to specific safeguards, including a comprehensive data protection regime for national use of the data (European Data Protection Supervision 2007, p. 5). The proposal initially envisaged that the regime regulating police access and processing of VIS data would be the purpose of the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. However, this Data Protection Framework Decision has, however, not yet been agreed.

To sum up, VIS is seen to be representing the latest effort in the EU's bid to establish "control over identity" as this system will register all visa applications and the fingerprints of the citizens of states that are required to request a visa when traveling to the EU (Guild 2003). Although it is hard to tell if this network of immigration databases actually constitutes a net that it will prove of success, as the amount of data stored is enormous and is set to grow at great speed, it is certain that the VIS database will become increasingly important in detection and identification of immigrants (Broeders & Engbersen 2007, p. 1605).

In a European context, the case for wider access to EU databases and their interoperability rests entirely in the vested interest of the police and other authorities for internal security. In a much quoted passage the European Commission explains that:

> In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as shortcoming. The same could also be said for SIS II and Eurodac data. This is now considered by the law enforcement community to be a serious gap in the identification of suspected perpetrators of a serious crime
>
> European Commission 2005

Plainly, the European Information Network is to be expanded at the request of the police. Indeed, combining and comparing data by a whole range of authorities in tandem with the open ended uses of biometrics at the European level might fundamentally challenge our conception of privacy and anonymity (Spokkereef 2008, p. 281). One of the main current concerns is the so-called Stockholm program, which will determine the EU plans for the next five years in the "Freedom, Security and Justice" area (European Commission 2009). In terms of data sharing, the Stockholm program aims at achieving full integration through total interoperability, and full access of databases for police purposes (European Commission 2009). The mantra henceforth has been that to combat terrorism and illegal migration it is inevitable that police and security authorities have access to EU's databases thus leaving concerns over proportionality and privacy unanswered (Baldaccini 2008, p. 46). This raises enormous privacy and security concerns and significantly intensifies the potential for surveillance and tracking of individuals. The challenging issues relate not simply to the tools like Eurodac that the EU developed to enhance its capabilities to combat international organized crime, including illegal migration, trafficking and terrorism. Rather, they concern the use and purpose of those tools (IOM 2003, p. 14). Anxiety grew over the exchange of biometric data, over who collates, stores, and accesses it and under what conditions for the individuals concerned? What legal framework should be implemented to protect individuals against the intrusion of these technologies in their private life? Could openness and accountability be guaranteed given the surrepticious expansion of Europol' remit to monitoring criminal activities, Eurodac, the Schengen information Systems and data sharing with third countries? (Lodge 2004, p. 266-267).

3.4 Conclusion

To conclude, it is evident that across the EU, biometric technology is being extensively deployed to demarcate and signify the identity of "non-citizens". This process is intertwined with the wider securitization of migratory flows and the attendant discursive "criminalization" of migrant identities (Wilson 2006, p. 101). Indeed many scholars argue that the introduction of biometric technologies in EU's migration policies serve to blend discourses of terrorism, organized crime and migration as a single coherent security threat (Redpath 2005, p. 16;Wilson 2006, p. 101). This is mostly evident in the case of E-passports where the EU undoubtedly has adopted a centralized surveillance approach in order to ensure an extensive control over peoples' movement. In the same context, the widening of the range of information available to the police and authorities responsible for internal security on persons who move, or seek to move, across borders is mainly seen in the development of EU's Information databases. Central repositories of this information, such as the Schengen Information System, the Visa Information System and Eurodac, are to be interlinked and opened up to police searches making millions of third-country nationals, whose personal data are recorded therein, vulnerable to potential misuses and abuses. Indeed, there is very little in terms of a safety net for foreigners to fall back on, should the assumptions as to the safety of the use of their data, accuracy and efficiency of the technology turn out to be misplaced. Although much will depend on the day-to-day use of these systems in the affairs of police, immigration officers and other authorities that have access to them, there are already rising concerns over the future implications of this ever expanding surveillance of population achieved through the development of EU's databases and e-passports. Therefore, it would now be important to examine the privacy and normative risks deriving from the EU's initiatives in migration management. There is a certain degree of friction between the security interests of policymakers and the right to privacy and free movement of those that are subjected to any of these measures. Because this friction is becoming central to the "biometric debate", civil libertarians are increasingly expressing their concern over potential social implications caused by the digitalization of EU's immigration policies as will be discussed in the next chapter.

Chapter 4

Digital Rule and Biometric Technologies in the EU:

A "surveillance threat" to civil liberties?

The digitalization of EU's borders and the introduction of biometrics in travel documents which is part of the EU's immigration strategy, does not only reveal the validity of the securitization thesis but also bring to light crucial questions over their possible impacts on civil liberties and rule of law. In fact, the EU is facing a difficult challenge in the attempt to establish itself as a new security actor and as a supranational democratic polity. Indeed, EU is currently taking important decisions in assuring that citizen's security is pursued on the basis of rule of law, respect of fundamental rights and democratic accountability (Liberatore 2005). However, the increasing digitalization and securitization that is currently taking place in the EU highlights the need for a better consideration of the potential social implications that derive from the extensive use of biometric applications in the migration/security context. Undoubtedly, the implementation of biometric technology in relation to border control will have a significant societal impact in the EU. The EU has a special responsibility both to its citizens and to its international partners to ensure the respect of the rule of law and the adherence to civil liberties.

Therefore this chapter will examine the practical and normative risks deriving from the use of biometrics in the field of migration. More specifically, the main objective is to identify both the functional and social implications of the current proliferation of identification practices based on biometric technologies and to encourage debate on the potential risks caused by the extensive use of biometrics in EU immigration policies. Hence, it will be important to push the debate on biometrics beyond the issue of "function creep" which is often used as a blanket term exhausting all further interest in uncovering potential dangers. Indeed, it is high time for further consideration of the implications for the rights to privacy and free movement of people as well as for a constructive debate on the potential "social profiling" and "digital discrimination" of individuals. To conclude, it will be argued that there is an increasing need and public demand for more transparency and accountability in the use of biometrics in the framework of EU's immigration

initiatives. For this to be achieved, the EU should not only seriously consider the implementation of stricter legal regulations but should also ensure in a decisive way the respect of fundamental rights and civil liberties.

4.1 Functional Dangers of Biometrics

It has been argued that the introduction of biometrics constitutes a fundamental change as it creates an "anchor" for identity in the human body, to which data and information can be fixed. This biometric anchor makes it conceivable to develop a global mechanism for government-sanctioned proof of identity (Spokkereef 2008, p. 279). However, trust in the reliability of the technology in making this anchor almost invulnerable to human mistake or fraud is mistaken (Spokkereef 2008, p. 279). It should be clear that there are in fact no such things as "infallible" biometrics (Schreiber 2007, p. 214). Even when the latter were the case, the safety of a system is only as strong as its weakest link, and therefore biometrics would still depend on total system safety. Therefore, the first section will examine the functional and rather practical risks deriving from the use of biometrics in he field of migration management.

To start off, one basic concern refers to the potential negative implications deriving from the function creep (Balzacq et al. 2008, p. 87). More specifically, the latter refers to the fact that biometric data collected for one purpose will be used for another functions without the consent of the individual (Lyon 2008, p.503). An example of this in the migration management context could be that data collected for immigration purposes is subsequently used for the prevention and detection of crime and regulation of access to state benefits (Redpath 2007, p. 10). Another illustrative example refers to EU's interest in further developing the functions of the European databases. More specifically, this initiative concerns the Commission's proposal for the creation of an agency to run the databases behind the second Schengen Information System (SIS II) on cross-border travel within the EU; the Visa Information System; and asylum seeker database EURODAC. The development of this "super-agency" brings to the front once again concerns over function creep and the negative implications that this may involve for the individuals (European Data Protections Supervisor 2009, p. 3). Indeed, in the absence of strict guidelines, and their enforcement, information collected could potentially be used for any number of activities. It is clear thus that once widely implemented the use of biometrics

could inevitably expand, both in the amount of data that will be collected and in the ways it will be used in everyday life (O'Neill 2005, p. 554). This is clearly an important issue, confronting the balance between liberty and security while reveal fears over the development of biometrics as "technologies of governance" of population mobility (Muller 2008, p. 208). Hence, such an approach is not only in contrast to the principles of data protection but is also socially unacceptable. If enforcement occurs without user consultation or choice, the result may be loss of confidence in, and a possible loss of respect for governmental agencies concerned (Ashbourn 2005, p. 16).

Having said that, it would now be important to underline the implications of function creep in the relations between citizens and the EU. Indeed, it may be true that, in the short term, citizens simply accept what many of them will see as the sacrifice of personal freedoms in order to support policies that they have been lead to believe will create a more secure world (Lodge 2004, p. 254). However, in the medium and longer term, the reality of the situation (such as it may be) may become self evident and, depending upon popular perception, this may lead to an erosion of trust which will not be in the interest of the European authorities (Liberatore 2007, p. 16). This is a very serious issue that should be taken fully into consideration with respect to current aspirations in the EU. Indeed, the EU should be in no doubt that it is tampering with the very fabric of society and should treat this fabric with the care and respect it deserves (Ashbourn 2005).

Furthermore, it is important to consider another potential danger deriving from the uncontrollable access to information contained in biometrics and databases. More specifically, the kind of information used in the development of biometrics may be used in a manner not permitted by law, whether by the authorized holder of the information or a third party (Redpath 2007, p. 12). In the context of third party access, computer systems used for the storage of biometric data are vulnerable to hacking and unauthorized use, as any other computer system, thus endangering to a great extent the security of the databases (Cholewinski 2007, 153). Hence, as many actors and control procedures are often involved in the use of biometric systems, not only are potentially several government authorities in a country entrusted with access to the data, but also increasingly private companies, such as airlines, which have a responsibility in the field of control of travel documents and security (Cholewinski et al. 2007, 154). As people should have control over their personal information, this is not the case when identifiable personal information is being collected without their knowledge and are being processed without their approval (Crompton 2002, p. 10). Given therefore the transnational nature of the migration/security

phenomenon, growth in the use of such systems and the likely expansion of actors having access to individuals' biometric information, consideration should be given to the establishment of national, European and indeed international, standards which ensure that the interests of the individual are adequately protected (Rejman-Green 2005, p. 343).

Finally, it must be noted that biometric systems are not infallible in performing either of these functions. The significance of this point in the migration/security context cannot be overstated, particularly as the industry is being forced to rapidly develop to meet the security demands of governments, and the fact that the international framework governing its use is evolving simultaneously with, and often in response to, the emergence of new technologies (Repath 2007, p. 14). Indeed, "the integrity of innocent citizens in the atmosphere of impossibility of error has to be protected under all circumstances" (European Parliament 2004, p. 17). Of particular concern is therefore the question of what happens to people who come up as a "hits" on the various databases, and how a "false hit" that leads to detention or deportation can be challenged (Amoore 2006, p. 340). More specifically, false acceptances (FAR) or false rejections (FRR) entail privacy risks as they may leave individuals in vulnerable positions such as in the case of denial access to services (Amoore 2006, p. 340). It is this preemptive fixing of identities that is emerging as a key point of contradiction and tension within the logic of biometric border, and is of central concern to advocacy groups, civil liberties and immigrant right groups. These organizations express their concern that these technologies are assumed to provide a complete picture of who someone is- leaving people having to dispute their own identity (Amoore & De Goede 2005, p. 162). Hence, the management of the border ceases to be a matter of geopolitical policing and discipline and becomes a matter of biopolitical management, while the border is seen as a "virtual site" through which the behaviours and daily practices of populations can be amendable to intervention and management (Amoore & De Goede 2005, p. 160).

Thus, an obvious objective for the use of biometric systems in migration management in the current security environment is to ensure a low level of false positives and the risk to be avoided is to treat as expendable the interests of a small percentage migrants (Redpath 2007, p. 33). Indeed, given the potential for refusing a visa or entry based on a false negative biometric reading, consideration should be given over ways to ensure an appropriate balance between the interests of the individual and the security needs of the state while assuring procedural fairness for the non-nationals in the migration process (Redpath 2005, p. 17). Having reviewed the functional dangers deriving from the

use of biometrics in the management of migratory flows it would now be important to examine their normative and social implications. Indeed, the examination of the functional risks cannot fully depict the gravity of the "biometric perils" and therefore this chapter will proceed to the examination of the privacy risks of biometrics on the individual level.

4.2 Biometrics and Privacy Risks

It is evident by now that the erosion between public and private sphere and the close connection between security and insecurity playing out in the space of the databases are constitutive characteristics of the politics of biometrics (Muller in Zureik & Satler 2005, p. 88). Indeed, biometrics has altered the way we are looking at the sphere of personal information as the political space of biometrics is becoming synonymous with the space of the dataset (Woodward 2003, p. 198). In the case of privacy, legality and broader socio-cultural concerns, the site of contestation is the database itself preoccupied with maintaining the integrity of the binary code and not the "integrity of the body". As a result, the sorts of issues that arise all assume the timeliness and practicality of biometrics, and indeed the way in which identity, security and liberty are already altered (Muller in Zureik & Satler 2005, p. 89).

To that extent, the literature on the privacy perils deriving from biometrics is becoming increasingly important. A sharp debate is emerging about whether biometric technology offers society any significant advantages over conventional forms of identification and whether it constitutes a threat to privacy and a potential weapon in the hands of authoritarian regimes (Mordini 2009, p. 239). At the heart of this academic debate, scholars have increasingly identified biometrics either as a friend or a foe of privacy. Indeed, while some argue that the use of biometrics such as in the case of travel documents is the answer to privacy threats deriving from identity theft (Schouten & Jacobs 2009), others remain rather critical and view their use as "the end of the free world" (Clarke 1991). Hence, biometric applications in the management of migratory flows are seen either as privacy enhancing technology or privacy intrusive technology.

4.2.1 Information Privacy and Bodily integrity

Before examining the various views over the use of biometrics in migration management and their potential implications for privacy it would be first of all important to define what we mean by privacy in this specific case. More specifically, David Banisar (2000) suggests that privacy can be divided in two separate but related concepts: first, the concept of information privacy that involves rules for the handling of personal data; and second bodily privacy that refers to the protection of our physical selves against invasive procedures. Indeed, both concepts are increasingly relevant in our examination of the social implications of biometric databases in migration management.

As far as the concept of information privacy is concerned, it is important to underline that predominately normative concerns are couched in terms of potential violations of privacy- a fundamental albeit not in all countries constitutional, legal, moral right. Data protection regimes such as those laid down in the European Directive on Data Protection (European Parliament and Council 2005) are morally and legally underpinned by reference to rights to privacy (Lyon 2003, p. 66). The object of protection is "personal data, that is, data pertaining to an individual in such a way that they are "identifying". The kind of privacy involved then is informational privacy that is defined in the ethical and legal literature as having control over somebody's data (Lyon 2003, p. 66).

As far as the concept of bodily privacy is concerned, Woodward argues that there are three core characteristics of this kind of privacy that should be taken under consideration: stigmatization, actual harm and hygiene (Woodward 2001, p. 23-26). Yet in relation to the generation and the storage of digital representations of individual bodily features, its relevance is considered in a very restricted way, if it is considered at all. For instance, in the context of biometric identification schemes, bodily integrity is discussed mainly with regard to the material contact of fingerprinting, DNA typing and various other forms of bodily searches used to generate biometrics. To that extent, the digital rendering of the bodies allows forms of processing, of scrolling through, of datamining aspects of a person's being in a way that endanger the integrity of the "machine-readable" body (Van der Ploeg 2005, p. 12).

Thus a specific division exists and reflects a particular ontological dichotomy: bodily integrity applies to "the thing itself" whereas informational privacy is presumed to cover all representations of it (Lyon 2003, p. 67). However, the capacity of the biometric

technologies to change the boundary, not just between public and private information but, also between what is inside and outside the human body, appears to blur the normative implications of the two concepts of privacy.

4.2.2 Biometrics as Privacy Enhancing Technology

Advocates of biometrics suggest that biometric technologies are "privacy's friends" as they can be used to protect information integrity and better identify theft (Woodward 2003, p. 199). Consequently, biometrics quickly seem to resolve the rivalry between liberty and security: it is in fact securing the database by protecting it from potential misuses/abuses of information; from the problem of functional creep where information is later used for purposes other than those originally intended; and from tracking, or the "Big Brother" fear, where anonymity and autonomy can no longer be maintained (Woodward 2001, p. 23-26). More specifically, advocates of biometrics as privacy enhancing technology argue that biometrics constitutes a potential solution to privacy problems by its potential to provide, for example, verification of identity in transactions and delivery of services without disclosing name, address, or other personal data (Van der Ploeg 2003, p. 88). Indeed, proponents of this position stress that biometric data do not contain much meaningful information, and that the irreversibility of the processing of biometric data into a template required by most systems prevents misuse. If, moreover, biometrics is combined with cryptographic techniques, it would be the strongest form of securing and protecting identities imaginable within today's technological possibilities (Van der Ploeg 2003, p. 88).

Hence, biometrics serve then in a "privacy friendly" role when they are used to safeguard identity, limit access to information and serve as privacy enhancing technology (Woodward 2003, p. 10). In the context of migration management, proponents of the introduction of biometrics in travel documents in tandem with the development of databases argue that biometrics will in due course be of great significance to the protection of privacy and the prevention of crime-terrorism and illegal immigration (Grijpink 2001, p. 12). As the advantages of using biometric systems in migration management include greater accuracy in ascertaining the identity of an individual and greater security in linking the document holder to this/her document, the individual's right to privacy is ensured (Redpath 2005, p. 15; Bruce 2009, p. 23). To sum up, biometrics

can be perceived as privacy's friend as the former can be used to protect information integrity and deter integrity theft. To that extent, the EU can play a positive role in regulating and thereby promoting public acceptance of this new technology by, for example, regulating ways that biometric information may be collected or disclosed (Woodward et al, 2003,p. 199).

4.2.3 Biometrics as a Privacy Intrusive Technology

On the other side, the critics of biometrics make various arguments as to how biometrics is "privacy's foe" (Liu 2008, p. 53). More specifically, biometrics is seen to be posing a threat to privacy since its use not only leads to loss of individual autonomy but also provides the state with a powerful ability and the appropriate "technologies of governance" to monitor the citizenry and migratory flows. To that extent, there are many concerns over the privacy threatening character of the use of biometrics which fall into the category of "information privacy" where the insecurity of the database is directly related to, and not divergent from, the concerns of liberty/privacy (Muller 2005, p. 89). Hence, a discourse of "inevitably crisis" is dominant in the debate about biometrics as identity/fraud and security from one side and freedom and privacy on the other side are constantly fluctuating (Muller 2004, p. 285).

Before examining the privacy intrusive nature of biometrics, it is important to clarify that privacy concerns relating to the general use of biometrics are equally applicable to their use in the migration/security nexus (Stalder 2002). To start off, one significant privacy risk of biometrics refers to the potential disclosure of further information of the subjects of biometric controls (Bolle et al. 2002, p. 2730). More specifically, biometric readings may divulge information about an individual in addition to his/her identity. Hence, the collection of information may reveal more information rather than just identity regardless of the intended use (Halperin et al. 2008, p. 77). Therefore, the concept of the "digital persona" coined by Clarke (1994) to capture how the enormous amount of personal data existing dispersed through databases and electronic networks, amounts to a kind of shadow identity of which the subject in question may be unaware, but which can be assembled into an extensive biography, find its meaning (Van Der Ploeg 1999, P. 42). It is evident that the issue of privacy becomes more serious with biometric-based recognition systems because biometric characteristics may provide

additional information about the background of an individual. For example, an iris scan may provide information on, for example, a person's state of health revealing thus the potential dangers deriving from the extensive use of biometric applications (Andronikou et al. 2008, p. 137).

Another privacy risk deriving from the deployment of biometrics refers to "the loss of anonymity-the loss of autonomy" of the individual (Woodward et al. 2003, p. 204). Indeed, some of the fears include that biometrics will also destroy anonymity. More specifically, a forceful critique of biometrics considers that there is no absolute anonymity especially when biometric information is used. (Nicoll, J.E.J. and Prins, M.J.2003). In representing "something you are", biometric modalities enable the ascription of fixed identities to individuals. As a result, the proliferation of biometric technologies in the EU could further limit an individual's ability to remain anonymous and therefore maintain his/her privacy in particular circumstances, for example, with regards to political affiliations, religious beliefs or sexual orientation (Liu 2008, p. 53).

Furthermore, another privacy risk that is directly linked to the practical dangers of biometrics concerns the questions over potential lack of interoperability at the international level. Given the international scope of the use of biometric systems in the migration/security context, their potential impact on an individual's right to privacy is compounded (Redpath 2007, p. 12). More specifically, migration/security management increasingly involves the prospect of large databases of biometric identification being gathered and exchanged throughout the world, where disparate standards for securing such databases exist and where principles of data and privacy protection apply unevenly (Redpath 2007, p. 12). Therefore, the current lack of absolute interoperability between all systems is often quoted as a source of privacy concerns and brings to the front potential negative implications of interoperable systems in the development of a surveillance society (Irish Council on Biometrics 2009, p. 74).

In addition, the European Parliament, some national Parliaments and advocacy organizations have been vocal in raising the issues of potential impacts of biometric identification technologies on privacy and data protection as well as their concerns over potential implications for human dignity and self-determination in relation to information (European Parliament 2004). Although the process of personal data protection and their potential transfer to third countries is closely associated with the functional risks of biometrics at the same time they offer a better understanding of the privacy risks of biometric databases. More specifically, privacy and data protection concerns are legally

framed by the directive of 24 July 1995.16 This directive is enacted to harmonize laws throughout the EU and to ensure consistent levels of protection for citizens and to allow for free flow of personal information inside the Union (Ceyhan 2008, p. 110). However, even if it constitutes a minimum level of protection, this directive is heavily criticized in two aspects. First, the nature of the data protected. Even if the directive does not make an explicit distinction between private and public data, it does not however provide a sound protection against governmental and security files which process personal information (Ceyhan 2005 in Bigo & Guild, p. 220). In effect, governments and security agencies succeed to bypass easily this provision for in practice, security files are often created in secrecy without prior declaration to the Data Protection Agency or Commissioner. It is often after their creation and enforcement (which may last a long time) that they adjust the privacy provision of their files to the EU criteria (Ceyhan 2008, p. 113). This raises crucial issues regarding the protection of the fundamental rights of individuals who are, as we mentioned earlier, almost unaware of the existence of such files that include personal information. Therefore, the increased risk of loss of control by the data subjects over their personal data consists one of the main critics over the privacy risks deriving from biometrics (Andronikou et al. 2008, p. 143). Indeed, biometric characteristics can be collected and processed in situations in which a data subject is not aware of and has no reason to believe that his personal data is being further processed (Andronikou et al. 2008, p. 144). A second aspect refers to the protection of individuals against the transfer of personal data towards third countries like the US (Ceyhan 2008, p. 110). Article 25 of the Directive stipulates that no data transfer towards third countries can be processed provided that these countries possess an "equivalent" data protection regulation. Considering the low-level of protection provided by the US framework which relies on the Privacy Act of 1974, the EU Commission had expressed reluctance about the transfer of the PNR data required by the DHS for authorizing the entry of airline travelers into the country (European Commission 2004). But the EU could not stand behind its refusal, because of the transformation of the PNR transfer into a condition for entering the American soil by air. Despite the criticisms addressed by the EU Parliament, the EU Commission signed an agreement with the US in 2006 authorizing the data transfer (European Commission 2006). Although both these concerns are closely related to the

technical and legal aspects of the use of biometrics, it is also evident that are closely associated to privacy risks as personal data are collected and accessed on an international level.

To sum up, the implementation of biometrics, whether secure and convenient or not, in the management of migratory flows raises great privacy-related fears. The new, intensive forms of monitoring, categorizing, scrutinizing and ultimately controlling of persons through their bodies and embodied identities that become possible in this new ontology of biometric technologies suggest that some form of informational and bodily privacy may be at stake (Lyon 2003, p. 71). In order to allay these concerns, a reinforced legal framework for privacy and data protection may be needed, one that adequately addresses the new technological possibilities of biometrics, thus preventing biometrics from becoming a tool in the service of surveillance. The particularly strong need for effective privacy and data protection provisions regarding biometrics reflects the fact that our biometric data are an inseparable part of us, whilst any document is merely an item at our disposal – there is nothing separating the individual and his/her biometrics (Maghiros et al. 2005, p. 116). Hence, privacy violations and other social costs result from such an undertaking may outweigh claims of efficiency and indeed security (Zureik & Hindle 2004, p. 120).

4.3 Social Sorting and "Digital Discrimination" in a Surveillance Society

It is evident by now that new surveillance technologies are forging up the traditional lines between national and international authority, foreign and domestic police, and intelligence gathering and criminal prosecution (Marx 2005, p. 25). With increased internationalization and globalization of terror, migration and social control (McDonald 1997;Deflem 2002; Sheptycki 2003), the meaning of borders is less clear. Under the present conditions, digitalization and computerization are making their mark on surveillance as information and communication technology has made it possible to link various databases and to create networks between them. (Gilliom 2001,p. 129). To that extent, the immigration databases developed in the EU are not an exception as they reflect the broader transformation of borders, control and surveillance. Indeed, the "potent"

combination of technological advances, the fear of terrorism and the consequent securitization of migration have facilitated many new surveillance programmes, uncovered existing ones and made new connections possible. (Lyon 2003, p. 92-94). Whether or not governments connect and combine different bodies of information is increasingly becoming a matter of legal constraints, as the technological constraints are losing their relevance quickly. However, the main effect of this technology will be a matter of changing methods rather than goals and intentions that in turn mainly concern the increasing surveillance of population movements.

In this globalized world of biometric surveillance, increased used of surveillance technologies such as the creation of immigrant databases and e-passports raise important concerns about the equality in its application of social control. These concerns mainly refer to the possibility of an excessive control over population movements while ignoring the social implications for both citizens and immigrants (Lyon 2003). Indeed, these new systems of surveillance echo the social need to control populations while remain closely related to social process of human decision making (Lyon 2003, p. 20). A forceful critique of biometrics and databases comes from David Lyon who argues that these surveillance technologies are designed and implemented to discriminate between social groups, to collect, categorize and evaluate (Lyon 2001, p. 10). Lyon refers to this process as social sorting. This concept of social sorting describes the different outcomes that result from categorizing groups of people, and suggests that "surveillance capacities are used to sort and sift populations, to categorize and to classify, to enhance the life chances of some and to retard those of others" (Lyon 2001, p. 4). Hence, the current methods of preemptive surveillance as manifested in the development of the European databases and e-passports have led to an increase in "social sorting" in which hierarchies of class, social position and race are increasingly instantiated in modern spaces (Salter 2005, p. 43).

Who you are, how you are, and how are you going to be treated in various situations, is increasingly known to various agents and agencies through information deriving from your own body, that is processed elsewhere, through the networks, databases of the information society (Ceyhan 2008, p. 114). Once translations of bodily characteristics into electronically processable data have been made, these bodies become amendable to forms of analysis and categorization in ways not possible before (Van der Ploeg 2005, p. 6). The biometrically identified bodies at an airport immigration booth are automatically assessed as either known or unknown, legal or illegal, wanted or unwanted, low or high risk security- assessments with very concrete consequences for the persons

concerned (Van der Ploeg 2007, p. 48). Particular profiles can be produced from large amounts of data and social identities affixed to persons without their knowledge, whether they actually fit the category in question or not (Van der Ploeg 2007, p. 49). With the growing interconnectedness of networks, cross-matching of databases, and sharing information between EU agencies and institutions such attributed identities can become like a person's shadow: hard to fight, impossible to shake (Van der Ploeg 2005, p. 12). Such practices of connecting social categorization and classification to the physicality of "machine-readable bodies" raise a number of ethical questions for example concerning discrimination and justice.

To that extent, as a social process, the entire system of surveillance-from the need to watch, to select, and code information to evaluating the information and the power imbued in the information output- reproduces social categories. Social categories of risk and social hierarchies allow judgements to be made about individuals and groups that include or exclude them from social, political or economic benefits (Lyon in Zurek & Satler 2005, p. 102). To that extent, social control is conducted through the deployment of the "technologies of governance" such as databases and biometrics. Hence, it is clear that the law-enforcement community has incorporated new surveillance technologies and capacities to facilitate its formal mandate of social control (Muller 2005, p. 98). This changing nature of social control has included developing and applying technologies to enhance surveillance, and has increased demands for improved cooperation within the law enforcement European community (Muller 2005, p. 98). Consequently, social control in a surveillance society rests upon the expanded capabilities of the member states authorities to collect, analyze and share information about population movements across international borders and between other national agencies whether or not these agencies were traditionally connected to law enforcement. Hence, surveillance will always be used for "social sorting", for the classification of populations as a precursor to differential treatment (Lyon, 2004, p. 142). Surveillance technology originating in EU cooperation will be no different.

In the context of the European databases, it is evident that the increasing securitization of migration and thus the "criminalization" of migrants and asylum seekers not only justify the extensive use of these databases beyond the reach of terrorist or criminal activities but also reveals the increasing social control that is currently taking place in the EU (Bigo 2005 in Bigo & Guild, p. 78). Indeed the de-localization of the control from the national border to a European locus has intensified the need to exercise

more control over migrant flows by the deployment of security technology (Bigo 2005 in Bigo & Guild, p. 81). In this environment, one of the questions that arises, refers to the technique of profiling that is increasingly used by the law enforcement agencies and the police (Ceyhan in Bigo & Guild 2005, p. 227). Based on Foucault's concept of "technologies of governance", social control and the consequent profiling is exerted through a continuous, uninterrupted process of supervision of the activities of people and in our case of migratory flows and is both the product and the means of accumulating knowledge about population movement. For instance, in the case of Eurodac, the question of whether it is acceptable to subject anyone to a greater level of surveillance than others in the population, will in turn foster discrimination and reinforce widespread prejudice still remains unanswered (European Parliamnet 2008). Indeed, measures which make it easier for police and other authorities to exchange information about individuals in respect of whom they have suspicions, which are insufficiently based on facts or evidence to justify coercive action, need to be carefully controlled to ensure that such exchanges do not result in indirect damage to the individual against whom there is nothing more than suspicion (Guild 2008, p. 190).

One of the main concerns deriving from the extensive exercise of social control is the risk of the profiling of migrants. More specifically, post 9/11 profiling has increasingly been institutionalized as a security measure (Tirman 2004, p. 225; Thobani 2003, p. 547). More specifically, profiling became to be seen as an acceptable political technique of governance through which suspicion and illegality is inscribed onto the bodies of immigrants (Thobani 2003, p. 598). This amplified and automated capacity to categorize and discriminate that attends biometric databases can only but deepen existing social divisions – already exacerbated through the profiling following the "war on terror" (Wilson 2006, p. 105). The social implications of this process of profiling reveal that immigrants are increasingly becoming the "ideal suspects" in a society where public anxiety for reassurance and security is being exacerbated and fulfilled through the deployment of unchallenged biometric databases. Hence, the capability of remotely granting or denying access through biometric technologies linked to databases undeniably contains the capacity to deepen and widen social discrimination (Wilson 2006, p. 92). Biometric technologies are then hastening processes of social discrimination were populations are digitally categorized as "worthy" and "unworthy", "included" and "excluded", "low-risk" and "high-risk" (Lyon 2003, p. 81). Hence, biometrics and their ability to authenticate and verify personal identity on the basis of behavioural and

physiological features are presented as desirable key elements in the categorization and processing of people such as immigrants raising in turn fears of using technology for social profiling purposes (Zureik & Hidle 2004, p. 116). Indeed, by using biology and physical appearance as means of identification, biometrics are likely to legitimize group differentiation and racialization in society in the name of security (Zureik & Satler 2004, p. 130).

Of course, the current focus on terrorism, provides the opportunity for government agencies to implement more stringent control via border control databases for a variety of reasons which have little to do with terrorism. The doctrine of exceptionalism, used to rationalize e-security, and the use of EU biometric databases to service immigration and internal security priorities such as combating terrorism may indeed compromise EU legitimacy and raises the spectre of citizens/migrants as suspects (Lodge 2004, p. 253). Hence, the integration of biometric databases allows the authorities to profile and encode people according to degrees of riskiness (Amoore & De Goede 2005, p. 162). The mastery of border risks by governments and their business and technology partners is undertaken on the back of the intensification and reallocation of risk onto the most vulnerable groups who experience even greater uncertainty in their lives (Amoore & De Goede 2005, p. 163).

To that extent, border control procedures currently operating in the European Union are becoming more extreme as authorities start profiling individuals and making assumptions based upon data such as name, ethnicity, or travel history which could result in discrimination or denial of service (Ashbourn 2004, p. 8). If large sectors of the population come to feel disenfranchised, discriminated against, subjected to unreasonable levels of surveillance, or treated like criminals then the development of these databases in the name of enhancing security will have the exact opposite effects as increasing numbers of migrants start to question the legitimacy of these databases (Ashbourn 2004, p. 14). It is evident that biometric measures have tended to discriminate against migrants deliberately as part of a policy to tackle illegal migration and as an unavoidable consequence of their contact with borders (Rebekah 2005, p. 3). In addition to this deliberate discrimination, immigrants and asylum seekers may also suffer disproportionately from the negative effects of biometric databases. The very act of collecting biometric information and the implications of such a procedure- the stigma of criminal activity- might be felt more acutely within different cultural groups. In the case of asylum seekers, such a procedure may not only be objectionable in principle, but may

be a terrifying and traumatic experience (Rebekah 2005, p. 3). Some critics of biometric application go further on their argumentation to suggest that these technologies are problematic as while they promise personal and national security not only they paradoxically increase social distinctions but they also succeed in criminalizing sections of the population such as asylum seekers (Wade 2004, p. 76).

Indeed, a view of surveillance from the point of view of the surveilled argues that, under certain conditions, surveillance can create a criminogenic environment that encourages distrust, stigmatizes innocent people, and may victimize those affected by it (Zureik & Hidle 2004, p. 118). Hence, in the EU, the concept of homeland security and its realization through the application of biometrics sit uncomfortably with the professed goals and values of the EU (Lodge 2004, p. 254). It is evident that the EU's security agenda reflects tension between the technical capabilities of e-governance and e-security and the political requirements of democracy and seems to side-step "freedom" and "justice" and to advance a "security" agenda that potentially compromises civil liberties (Lodge 2004, p. 254).

4.4 Conclusion

To conclude, it is evident that the systematic monitoring of individual's personal data through the application of information technologies- datasurveillance -is becoming the rule in the management of migratory flows in the EU. With these technologies, surveillance extends beyond the immediate gaze associated with direct monitoring and becomes more and more "automated, dispensing as far as possible with human operatives" (Lyon 2003, p. 63). What is worrying though is the fact that the surveillance of population movements authorize an ever widening sphere of actors and practices to engage in surveillance and policing of migratory flows while leaving untouched privacy concerns (Amoore 2006, p. 346). To that extent, it is clear that while biometrics have the potential to benefit individuals and society through its privacy enhancing capabilities, it is also very clear that the potential risks to privacy such as bodily integrity, reveal tensions that need to be adequately addressed by the legal community.

Regardless from these concerns that currently dominate the debate on the use of biometrics in EU's immigration policies, it is important to notice that in the age of "war on terrorism", vulnerable groups, minorities and immigrants are at the centre of a process

of social sorting and profiling, where "technologies of governance" have a crucial role in the process of a social categorization. More specifically, there are significant concerns about the way in which biometric databases rely on and reinforce the categorization of certain sociospatial risk categories such as immigrants. For these concerns to be convincingly addressed, the legal framework of the "EU data surveillance architecture" is highly important not only for the protection of individual rights, but also for the legal framing and prevention of "digital discrimination and social sorting" against immigrants (Brouwen in Balzacq & Carrera 2006 p, 153). Hence, there is a need for strong legal protection including appropriate mechanisms of accountability in order to effectively hamper the normative and ethical implications of biometrics in the EU.

Conclusion

Starting from a longstanding personal unease with the way migration has been transformed into a security issue within the EU during the last decades, this dissertation offers satisfactory answers to the increasing securitization and digitalization of migration management in the EU. Indeed, the recent politicization of migration and asylum in a security framework, in tandem with the increasing deployment of "technologies of governance" to "survey" population movements, have come to dominate the debate on the development of EU's databases and the introduction of biometrics in EU's travel documents.

To that extent and building up from the "securitization discourse" of the Copenhagen school as well as from Foucault's notion of "technologies of governance", this dissertation attempts to tackle issues arising from the increasing digitalization of EU's immigration policies. In line with the "securitization thesis", various attempts to explore the destabilizing effects of migration in the political, economic and social realm of the European countries through the identification of migration issues as a security threat, offer ample legitimacy to the introduction of biometric technologies in EU's e-passports as well as to the development of EU's databases. Indeed, the driving force behind EU's initiatives has been entirely political and is aimed at proving some sort of successful response to terrorism and other security concerns. To that extent, it is maintained that the EU's current approach to informational trends and biometrics could be proven rather beneficial in responding to the "political constructed" security threats deriving from migratory flows. Concurrently, however, these initiatives are also being viewed as technologies developed "to categorize the individual, to mark him by his own individuality, to attach him to his own identity and to impose a law of truth on him which he must recognize and which others have to recognize in him" (Foucault 2000a, p. 328). To that extent, the increasing introduction of biometrics in travel documents and the development of EU's databases such as the Schengen Information System and Visa Information System are criticized as being micro techniques of discipline that target and treat the body as an object to be watched, assessed and even manipulated.

It is clear that while the EU is progressively establishing itself as a new security actor, the nature of such "actorness" is still unclear as normative and ethical concerns of its current digitalization have come to challenge the legitimacy of EU's initiatives.

Indeed, serious concerns arising from the very nature of biometrics as well as from the lack of a clear perspective on the ever-increasing digitalization of borders in the EU reveal the need for ensuring an appropriate balance between the interests of the individual and the security anxieties of the EU. Concerns over the lack of openness and the potential privatization of control over the storage of personal data raise serious questions about accountability, the relationship between the EU and citizen, and the evacuation of genuine meaning of civil liberties in the EU.

From a more explicitly normative standpoint, then, it has been suggested that the development of a surveillance society is currently taking place partly due to the pace and pervasiveness of technological change and partly due to the influence of security concerns and discourses. Concerns over the "privacy intrusive" nature of biometrics, in tandem with risks deriving from the lack of adequate legal constraints and provisions, further accentuate the social implications and fears over the digitalization of EU's databases. However, the most prominent threats deriving from these EU's initiatives refer mainly to the potential "social sorting" and "digital discrimination" effects of the optimization of surveillance technologies. Indeed, surveillance today is seen as sorting people into categories and assigning worth of risk through a process of extensive social control and with detrimental effects for the individuals concerned. To that extent, discrimination occurs, thus making surveillance not merely a matter of personal privacy but social justice (Lyon 2003).

It is evident that there is an increasing need for strengthening accountability and ensuring the full respect of civil liberties in the development and implementation of these EU's initiatives. Indeed, the EU's approach to informational trends and biometrics needs to be developed towards a more comprehensive notion of societal protection through the deep consideration of the society as a whole. The staring point then should be a re-focusing of objectives and an acknowledgement of the social implications of biometrics in EU's migration management while offering a clearer perspective on the specific functions and processes involved in the development of EU's databases. To conclude, then, there is a need for a fruitful public debate not only based on political aspirations but entailing genuinely consultations with citizens in order to ensure full accountability and transparency in the EU's digital initiatives.

Bibliography

Primary Resources

- European Commission 2000. *Initiative of the Grand Duchy of Luxembourg with a view to the adoption of a Council Decision establishing a procedure for amending Articles 40(4) and (5), 41(7) and 65(2) of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders.*, Available at: http://ec.europa.eu/justice_home/doc_centre/police/schengen/doc_police_schengen_en.htm
- European Commission 2003. *Commission proposal for a Regulation on biometrics documents,* 29 September 2003. Available at: www.euractiv.com/en/.../**biometrics**...**documents**/article-132063
- European Commission. 2004. *Free Movement within the EU- a fundamental right.* Available at: http://ec.europa.eu/justice_home/fsj/freetravel/fsj_freetravel_intro_en.htm
- European Commission. 2005a. *Biometrics and Justice.* No 46, August 2005.Available at: http://ec.europa.eu/research/rtdinfo/46/article_2932_en.html
- European Commission 2005b. Council conclusions on biometric data, 24 February 2005. Available at: http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_en.htm
- European Commission 2006, *EU-Passport Specification Working Document,* 28 June 2006. Available at: www.ec.europa.**eu**/justice_home/doc_centre/.../c_**2006**_2909_en.pdf
- European Commission 2008, *Border Package- facilitating travel and securing Europe's borders*. Available at: http://ec.europa.eu/justice_home/news/information_dossiers/borders_08/index_en.htm
- European Commission 2009. *European Commission outlines its vision for the area of freedom, security and justice in the next five years.* Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/894

- European Council. 2003. *President Conclusions. Thessaloniki European Council.* 19 and 20 June 2003. Available at: www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/.../76279.pdf
- European Council 2004a. *Action Plan on the Hague Programme 16054/04.* Available at: *ec.europa.eu/justice_home/doc_centre/.../**hague_programme**_en.pdf*
- European Council. 2004b *Declaration on Combating Terrorism* Available at: http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/ec/79637.pdf
- European Council 2007. *Council Document 5291/07.* 12 January 2007. Available at: www.*web.mvcr.cz/archiv2008/eunie/.../de_program_18_month_cats.pdf*

Secondary Resources

- Abid Mohamed and Afifi Hossman, 2009.”Towards a secure E-passport protocol based on biometrics”,*Journal of Information Assurance and Security* 4: 338-345
- Alterman. Anton, 2003. “A piece of yourself: Ethical issues in biometric identification” *Ethics and Information Technology* 5: 139-150
- Amoore, Luise and De Goede, Marieke 2005, ”Governance, risk and dataveillance in the war on terror”, *Crime, Law & Social Change* 43: 149-173
- Amoore, Luise 2006. “Biometric Borders: Governing mobilities in the war on terror”, *Political Geography* 25: 336-351
- Andronikou, Vassiliki Angelos Yannopoulos and Theodora Varvarigou 2008, in Hildebrandt Mireille and Gutwirth Serge, *Biometric Profiling: Opportunities and Risks,* Netherlands: Springerlink
- Ashbourn, Julian 2000. *Biometrics: Advanced Identity Verification. The Complete Guide,* UK: Springer
- Ashbourn, Julian, 2004. *Practical Biometrics: From aspiration to Implementation.* London: Springer-Verlag.
- Baldaccini, Anneliese. 2008. “Counter-Terrorism and the EU Strategy for Border Security: Framing Suspects with Biometric Documents and Databases”, *European Journal of Migration and Law* 10: 31-49
- Banisar David, 2000, *Privacy and Human rights: an international survey of privacy laws and developments*, Electronic Privacy Information Centre, Washington
- Bigo, Didier. 1996 *Polices en Réseaux: L’expérience Européenne.* Paris: Presses de Sciences Po

- Bigo, D., Bonelli, L., Guittet, E., Olsson, C. and Tsoukala, A. eds 2006. *Illiberal Practices of Liberal Regimes: The (In)security Games.* Paris: L'Harmattan
- Bigo, Didier 2002. "Security and Immigration: Toward a Critique of the Governm
- Bigo, Didier. "Frontier Controls in the European Union: Who is Control?" in Bigo, Didier & Guild Elspeth, 2005. *Controlling Frontiers. Free Freedom into and within Europe",* USA: Ashgate Publications Limited
- Blake, Nicholas 2003." Exclusion form Refugee Protection: Serious Non-political Crimes after 9/11", *European Journal of Migration and Law* 4, no. 4: 425-447
- Broeders, Dennis and Engebersen, Godfried 2007. "The Fight against Illegal Migration: identification Policies and Immigrants Counterstrategies". *American Behavioral Scientist* 50: 1592−1609.
- Bolle, Ruud M., Nalini K. Ratha and Sharath Pankanti. 2004. "Error analysis of pattern recognition systems - the subsets bootstrap." *Computer Vision and Image Understanding* 93, no. 1: 1-33.
- Boniface, Jérôme, Wesseling, Mara, O'Connell, Kevin, Ripoll Ariadna. 2008. "VISA Facilitation versus Tightening of control: Key aspects of the ENP". Available at: www.eipa.eu/files/**visa_facilitation**.pdf
- Boswell, Christina. 2007 'Migration control in Europe after 9/11" explaining the absence of securitization', *Journal of Common Market Studies* 45, no 3: 589-610
- Boswell, C. "Migration, Security and Legitimacy" in Givens, T. E., Freeman, P. G., Leal, L. D. 2009, *Immigration Policy and Security. U.S., European and Commonwealth Perspectives,* New York: Routledge Taylor & Francis
- Broeders, Dennis 2007."The new digital borders of Europe. EU Databases and the surveillance of irregular migrants, *International Sociology* 22, no. 1: 71-92
- Broeders, Dennis 2009a. *Breaking Down Anonymity. Digital Surveillance on irregular migrants in Germany and the Netherlands*. Netherlands: Amsterdam University Press
- Broeders, Dennis and Engbersen,Godfried 2009b. "The State versus the Alien: Immigration Control and Strategies of Irregular Migrants", *West European Politics* 32, no, 5: 867-885
- Balzacq, T., Bigo, D.,Carrera, S & Guild,E. 2006. "Security and the two-level game: The treaty of Prum, the EU and the management of threats" *CEPS Working Document, no. 234/January 2006.*

- Brouwer, E. 2002. “Eurodac: its limitations and temptations”, *European Journal of Migration and Law* 4: 231-247
- Brouwer, E. (2006) ‘Data Surveillance and Border Control in the EU: Balancing Efficiency and Legal Protection’. In Balzacq, T. and Carrera, S. (eds) *Security Versus Freedom?: A Challenge for Europe’s Future* (Aldershot: Ashgate).
- Buonfino, A. (2004). "Between unity and plurality: the politicization and securitization of the discourse of immigration in Europe." *New Political Science* 26, no. 1: 23-49.
- Schneier Bruce, 2009. “New Frontiers on Biometrics”. Available at: *www.schneier.com/blog/archives/**2009**/.../new_frontiers_i.html*
- Buzan, Bary1991. *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era.*
- Buzan, Bary Waever Ole and De Wilde, Jaap. 1998.*Security. A new Framework of Analysis,* USA: Lyne Rienner Publishers
- Barry Buzan and Ole Wæver, Regions and Powers: The Structure of International Security, Cambridge University Press 2003.
- Cambell, David1992. *Writing Security. United States Foreign Policy and the Politics of Identity.* Minneapolis: University of Minnesota Press
- Castells, M 1996. *The Information Age. Economy, Society and Culture. Volume i: The Risk of the Network Society,* Oxford: Blackwell Publishers
- Ceyhan, Ayse 2008. “Technologization of Security: Mangement of Uncertainty and Risk in the Age of Biometrics”, *Surveillance & Society* 5, no. 2: 102-123
- Ceyhan, A. and Tsoukala, A. (2002) “The Securitization of Migration in Western Societies: Ambivalent Discourses and Policies”. *Alternatives* 27, no. 1: 21-39.
- Cholewinski, R. 2000. "The EU acquis on irregular migration: reinforcing security at the expense of rights." *European Journal of Migration and Law* 2: 341-405.
- Cholewinski, Ryszard, Perruchoud, Richard and MacDonald, Euan. 2007. *International Migration Law. Developing Paradigms and Key Challenges.* UK: Asser Press
- Clarke, R.A. 1988 “Information Technology and Dataveillance,” *Communications of the ACM,* 31: 29-45.
- Crompton, Malcolm. 2002.” The End Of The World as We Know It Or The White Knight Of Privacy” *Australian Journal of Forensic Sciences* 2: 49 - 58

- Davis, Darren W. and Silver D. Brain. 2004. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks in America." *The American Journal of Political Science* 48, no.1: 28-46.
- De Hert Paul 2005. "Biometrics: legal issues and implications" *Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission:* 1-39
- De Hert Paul 2006 "Interoperability of Police Databases Within the EU: An Accountable Political Choice?" *Tilburg University Legal Studies Working Paper No. 003/2006:* 21-35
- Deflem, M. 2002. *Policing world society: Historical foundations of international police cooperation.* Oxford; New York: Oxford University Press.
- Deflem, Mathieu and Shutt, J. Egle 2006. "Whose Face at the Border? Homeland Security and Border Policing since 9/11". *Jpurnal pf Social and Ecological Boundaries* 1, no. 2: 81-105
- Dhian Ho, Monika Sie 2004. "Enlarging and Deepening EU/Schengen Regime on Border Controls*", paper presented at `Workshop on Managing International and Inter-Agency Cooperation at the Border`, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Genève*
- Eliott, John 2009."Going Mobile". *Biometric Technology Today* 9, no. 4: 7-9
- H. Fassmann, M. Haller & D. Lane 2009 *Migration in Europe – Threat or Chance.* Cheltenham: Edward Elgar
- M Foucault, LH Martin, H Gutman,1988. *Technologies of the self. A seminar with Michel Foucault" ,* The University of Massachusetts Press
- Foucault, Michel, 1991. "Governmentality"|, in *The Foucault Effect: Studies in Governmentality.* G. Burchell, C. Gordon and P. Miller (Eds.) London: Harvester Wheatsheaf.
- Foucault, Michel 1997. In Rabinow, P., ed. *Michel Foucault: Ethics Essential Works of Foucault 1954-1984,* Vol. 1. London: Penguin Books
- Foucault, Michel 2000 "The Ethics of the Concern of the Self as a Practice of Freedom", in Rabinow, P., ed. *Michel Foucault: Ethics Essential Works of Foucault 1954-1984,* Vol. 1. London: Penguin Books

- Foucault, Michel 2004, *'Society must be defended': lectures at the College de France, 1975–76*, trans. D Macey, Penguin Books, London.
- Graham Stephen and Wood David, 2003. "Digitizing surveillance: categorization, space, inequality" *Criticial Social Policy* 23, no. 2: 227-248
- Grijpink, J.H.A.M. (2008). Trend report on biometrics: Some new insights, experiences and developments. *Computer Law and Security Report, 24*, no. 3: 261-264.
- Guild, Elspeth. 2001."Moving the Borders of Europe", *Inaugural Lecture at the University of Nijmegen:* 1-72
- Guild, Elspeth. 2003 'International terrorism and EU immigration, asylum and borders policy: the unexpected victims of 11 September 2001', *European Foreign Affairs Review* 8: 331-346
- Guild, Elspeth 2008, "The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the "Terrorist Lists". *Journal of Common Market Studies* 46, no. 1: 173-193
- Guild Elspeth, Carrera, Sergio and Geyer, Florian 2008. "The Commission's New Border Package: It take us one step closer to a "Cyber-Fortress Europe? CEPS Policy Brief No. 154, March 2008.
- Available at SSRN: http://ssrn.com/abstract=1334058
- Guirandon, V. 2000, "European Integration and Migration Policy: Vertical Policy Making as Venue Shopping", *Journal of Common Market Studies* 38, no. 2: 251-271
- Haggerty, K. & R. Ericson (2000) 'The surveillant assemblage', *British Journal of*
- *Sociology* 51, no 4: 605-622.
- Halperin Ruth and Backhouse, James. 2008. "A roadmap for research on identity in the information society" *Identity in the Information society Journal* 1, no. 1:71-87
- Heisler, Martin O. and Zig Layton-Henry 1993, "Migration and the Link between Social and Societal Security," in Ole Waever, Barry Buzan, Morten Kelstrup and Pierre Lemaitre, eds. *Identity, Migration and the New Security Agenda in Europe*, London: Frances Pinter
- Redpath, Jullyanne. 2005. "Biometrics and International Migration". *International Migration Law*. No. 5, *International Organization for Migration* : 5-17.

- Richard Hopkins.1999. “An Introduction to Biometrics and Large Scale Civilian Identification”. *International review of law, computers and technology* 13, no. 3: 337-363
- Huysmans, Jef 1994, “The Migrant as a Security Problem,” in Robert Miles and DietrichThränhardt, eds., *Migration and European Integration: The Dynamics of Inclusion and Exclusion*, London: Pinter
- Huysmans J. 2000. “The European Union and the securitization of Migration”, *Journal of common market studies* 39. no 5: 751-777
- Huysmans 2006, *The politics of Insecurity. Fear, Migration in the EU,* Routledge:
- LondonIOM 2003,
- Huysmans, Jef and Buonfino, Alessandra 2008, “Politics of Exception and Unease: Immigration, Asylum and Terrorism in Parliamentary Dbeates in the UK”, *Political Studies* 56: 766-788
- Irish Council on Biometrics 2009,Biometrics. Enhancing Security or Invading Privacy?”, Published by The Irish Council for Bioethics, Dublin, pp. 1-192
- Jain AK, Ross A and Prabhakar S 2008. “An Introduction to Biometric Recognition”|. *IEEE Transactions on Circuits and Systems for Video Technology* 14, no. 1: 4–20.
- Jones, M. (2007), "An Introduction to Political Geography Space, Place, and Politics". New York: Routledge
- Karyotis, G. 2007, “European Migration Policy in the Aftermath of September 11.
- The security-migration nexus”, *Innovation,* vol. 20, no. 1, pp. 1-14.
- Kruelle, Grace,. Swatman, Paul A , Hampe, J. Felix 005, “Biometrics and E-identity (e-passport) in the European Union: Overcoming Poc-cultural diversity for common cause?, *IADIS International Conference e-Society,* 537-541
- Kumar B.V.K. Vijaya Kumar and P.K. Khosla, Marios Savvides, “*Cancelable Biometric Filters For Face Recognition*”, International Conference of Pattern Recognition, ICPR 2004, Cambridge.
- Léonard, S. 2004 "Studying Migration as a security issue: conceptual and methodological challenges."*Paper presented at the SGIR Fifth Pan-European International Relations Conference, the Hague* , 9-11 September
- Leonidou, Iris 2002.” Iris Scan: Closer than we think?,*GIAS Security Essentials Certification No. 1.4b,* pp. 3-19

- Lewis, Nancy. 2005.” Expanding Surveillance: connecting biometric information systems to international police cooperation” in Zureik, Elia and Salter, B. Mark 2005, *Global surveillance AND policing. Borders, Security, Idntity,* UK: Willan Publication
- Liberatore, Angela. 2005.”Balancing Security and Democracy: The Politics of Biometric Identification in the European Union, *European Union Institute Working Paper No. 20005/30:* 1-29
- Liberatore, Angela 2007. “Balancing Security and Democracy: The Politics of Biometric Identification in the European Union”, *European University Institute RSCAS NO. 30:* 4-23
- Liersch, Ingo 2009. “Electronic Passports- from secure specifications to secure implementations” *Information Decurity Technical Report* 14: 96-100
- Liu, Yue 2008. “Identifying Legal Concerns in the Biometric Context” *Journal of International Commercial Law and Technology,* 3, no. 1: 1-10
- Lodge, Juliet. 2004. “EU Homeland Security: Citizens or Suspects?”, *European Integration* 26, no. 3: 253-279.
- Luetdke Adam, 2009, “Fortifying Fortress Europe? The Effect of September 11 on EU immigration policy” T. E., Freeman, P. G., Leal, L. D. 2009, *Immigration Policy and Security. U.S., European and Commonwealth Perspectives,* New York: Routledge Taylor & Francis
- Lyon, David 2003. *Surveillance as Social Sorting. Privacy Risk and Digital Discrimination.* New York: Routldege
- Lyon 2004 “New directions in theory,” in Frank Webster (ed.) *The Information Society Reader*, London and New York: Routledge, 2004. (reprinted from *Surveillance Society*, Open University Press, 2001)
- Lyon, David 2008. “Biometrics, Identification and Surveillance”, *Bioethics* 22, no.9: 499-508
- Maghiros Ioannis, Yves Punie, Sabine Delaitre, Elsa Lignos, Carlos Rodríguez, Martin Ulbrich, and Marcelino Cabrera. Bernard Clements, Laurent Beslay, and Rene van BavelMäkinen 2005. “Biometrics at the Frontiers: Assessing the Impact on Society”. *Paper prepared for the European Parliamnet Committee on Citizens’ Freedoms and Rights, Justice and Home Affairs (LIBE):* 1-166

- McSweeney, B. (1999) *Security, Identity and Interests: A Sociology of International Relations,* Cambridge: Cambridge University Press.
- Mitsilegas, V., J. Monar & W. Rees (2003) *The European Union and internal security. Guardian of the people?* Houndmills, Basingstoke, Hampshire: Palgrave.
- Mitsilegas, Valsamis 'Border Security in the European Union: towards centralised controls and maximum surveillance', in A. Baldaccini, E. Guild and H. Toner (eds), *Whose Freedom, Security and Justice? EU Immigration and Asylum Law*, Hart Publishing, 2007.
- Mitsilegas, Valsamis, 2009 "Borders, Security and Transatlantic Cooperation in the Twenty-First Century: Identity and Privacy in an Era of Globalized Surveillance" Givens, T. E., Freeman, P. G., Leal, L. D. 2009, *Immigration Policy and Security. U.S., European and Commonwealth Perspectives,* New York: Routledge Taylor & Francis
- Mordini E and Massari S 2008. "Body, Biometrics and Identity". *Bioethics* 22(9): 488–498.
- Muller J. Benjamin 2004 "Borders, bodies and biometrics" towards identity management" in Zureik & Satler Zureik, Elia and Salter, B. Mark 2005, *Global surveillance AND policing. Borders, Security, Idntity,* UK: Willan Publication
- Newland, K., Patrick, E., van Selm, J. and Zard, M. (2002) 'Introduction', *Forced Migration Review*, 13 4–7.
- Nicoll, J.E.J. Prins, M.J.M. (2003), Digital Anonymity and the Law: Tensions and Dimensions / ed. by C. Nicoll, J.E.J. Prins, M.J.M van Dellen. The Hague: Asser Press.
- O'Neil, Patrick 2005, "Complexity and Counterterrorism: Thinking about Biometrics" *Studies in Conflict & Terrorism* 28, no. 6: 547-566
- Pap, András 2008, "Ethnicity and Race-Based profiling in Counter –Terrorism, Law Enforcement and Border Control" *CEPS: pp. 1-63*
- Pickering, Sharon and Weber, Leanne 2006 *Borders, Mobility and Technologies of Control",* Netherlands: Springer
- Pickering, S. (2004) 'Border Terror: Policing, Forced Migration andTerrorism', *Global Change, Peace and Security*16: 3: 211–26.
- Rejman-Green,M. 2005 "Security considerations in the use of biometric devices'", *Information Security Technical Report*, 3, No 1: 77-80

- Ross, Arun & Jain, Anil 2003,"Information Fusion in Biometrics" *Pattern Recognition Letters* 24, no. 13: 2115-2125
- Rudolph, C. (2006) *National Security and Immigration*. Stanford CA: Stanford University Press.
- Sarkar S and Liu Z (2008). Gait Recognition. In AK Jain, P Flynn and AA Ross (eds.) *Handbook of Biometrics*, Springer, New York, p.109–129.
- Saux, Maria Soledad 2007."Immigration and Terrorism: A constructed Connection. The Spanish Case". *European Journal Criminal Policy,*
- Schouten, Ben and Jacobs Bart 2009, "Biometrics and Their Use in E-passports", *Image and Vision Computing* 27: 305-312
- Schreiber, Wolfgang, 2007, "Biometrics-Applications, Costs and Risks". *Regio-Minorities, Politics, Society* 1: 207-216.
- Sheptycki 2003
- Sparke, B. Matthew, "A neoliberal nexus: Economy, security and the biopolitics of citizenship on the border", *Political Geography* 25: 151-180
- Spinella, Edmund 2003. "Biometric Scanning Technologies", *SANS Institute :* 1-15
- Sprokkereef, Annemarie 2008, "Data Protection and the Use of Biometric Data in the EU" *International Federation for Information Processing,* 262: 277-284
- Stivachtis Yannis, 2008 "International Migration and the Politics of Identity and Security", *Journal of Humanities and Social Sciences* 2, 1: 1-24
- Thobani, S., 2003, Exception as rule: profile of exclusion, *Signs: Journal of Women Culture and Society*, 29, no. 2: 597–600.
- Tirman John 2004, *The maze of fear: Security and Migration after 9/11.* Ney York: The New Press
- Toprey J. 2000, *The Invention of the Passport. Surveillance, Citizenship and the State.* Cambridge: Cambridge University Press
- Van der Ploeg, Ian., 1999a, "The illegal body: 'Eurodac' and the politics of biometric identification", *Ethics and Information Technology*, 1: 295–302.
- Van der Ploeg, Ian., 1999b, "Written on the body: biometrics and identity", *Computers and Society*, 29, no. 1: 37–44
- Van der Ploeg, Ian.,2003, "Biometrics and privacy: a note on politics of theorizing technology", *Information, Communication and Society* 6, no. 1: 85–104.

- Van der Ploeg, Ian 2005. *Biometric Identification Technologies: Ethical Implications of the Informatization of the Body*. BITE Policy Paper No.1. 18p. Available online at:
- http://www.biteproject.org/documents/policy_paper_1_july_version.pdf,
- Van Dijk, Dominique 2006, "Is the EU policy on illegal migration securitized? Yes of course! A study into the dynamics of institutionalized securitization". Paper to be presented at the 3rd Pan-European Conference on EU Politics,Istanbul: 1-32
- Wade Lindsay 2004,"Facing the threat: Invading the body for national security" *Knowledge, Technology, Policy* 17, no. 1 : 74-80
- Waever Ole 1995, "Identity, Integration and Security: Solving the Sovereignty Puzzle in EU studies", *Journal of International Affairs,* 48, no.: 389-431
- Walters, W. 2002 'Deportation, Expulsion, and the international police of aliens', *Citizenship Studies* 6, nr. 3, pp. 265-292
- Welch, M. and Schuster, L. 2005 'Detention of Asylum Seekers in the UK and USA', *Punishment and Society*, 7 no. 4: 397–417.
- Wilson Dean 2006. "Biometrics. Borders and the Ideal Suspect", *Borders, Mobility and Technologies of Control*: 87-109
- Woodward D. John, Orlans M. Nicholas and Higgins, T. Peter 2003, *Biometrics. Identity Assurance in the Information Age".* California: McGraw-Hill
- Zuriek, Elia. and Hindle, K., 2004, "Governance, security and technology: the case of biometrics", *Studies in Political Economy*, 73: 113–137.
- Zureik, Elia and Salter, B. Mark 2005, *Global surveillance AND policing. Borders, Security, Idntity,* UK: Willan Publication